KOCAELİ ÜNİVERSİTESİ * FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL GÖRÜNTÜLER İÇİN HİSTOGRAM TEMELLİ VERİ GİZLEME YÖNTEMİ VE UYGULAMA YAZILIMI

DOKTORA TEZİ

Yıldıray YALMAN

Anabilim Dalı: Elektronik ve Bilgisayar Eğitimi

Danışman: Prof. Dr. İsmail ERTÜRK

KOCAELİ, 2010

KOCAELİ ÜNİVERSİTESİ * FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL GÖRÜNTÜLER İÇİN HİSTOGRAM TEMELLİ VERİ GİZLEME YÖNTEMİ VE UYGULAMA YAZILIMI

DOKTORA TEZİ

Yıldıray YALMAN

Tezin Enstitüye Verildiği Tarih: 17 Haziran 2010

Tezin Savunulduğu Tarih: 15 Temmuz 2010

Tez Danışmanı
Prof. Dr. İsmail ERTÜRK
(.....)

Üye
Doç. Dr. Yunus Emre ERDEMLİ
(.....)

Üye
Doç. Dr. Celal ÇEKEN
(.....)

Üye
Yrd. Doç. Dr. İbrahim ÖZÇELİK
(.....)

Üye
Yrd. Doç. Dr. Özdemir ÇETİN
(.....)

KOCAELİ, 2010

ÖNSÖZ VE TEŞEKKÜR

Günümüz teknolojisinin baş döndürücü şekilde gelişmekte olması, bilgi ve bilginin korunması konularını ön plana çıkarmıştır. İnsanlık tarihi ile neredeyse aynı geçmişe sahip olan gizli haberleşme gereksinimi teknolojinin gelişimi ile birlikte sürekli şekil değiştirmekte ve önemini gün geçtikçe arttırmaktadır. Veri gizleme bilimi, tarihsel gelişimine bakıldığında, genellikle askeri amaçlar için kullanılmıştır. Ancak bilgisayar kullanımının artması ile birlikte her evin içerisinde dünyaya açılan bir kapı bulunmakta ve mesafeler hızla ortadan kalkmaktadır. Bu nedenle bireylerin kişisel bilgilerini gizleme gereksinimi son yıllarda oldukça önem kazanmıştır. Gün geçtikçe gelişen iletişim ortamında, özel hayatın mahremiyetini ve insanların aralarındaki haberleşme güvenliğini sağlamak neredeyse imkânsız hale gelmiştir. Günümüzde araştırmacılar, çok çeşitli sayısal ortamları kullanarak veri gizleme yöntemleri geliştirmişlerdir. Bu noktada öne çıkan, geliştirilen yöntemin hangi sayısal ortam üzerinde uygulandığından çok, fark edilebilirliğidir. Sadece veri gizlenmesi değil, gizlenen verinin üçüncü kişiler tarafından tespit edilmesini önleyecek mekanizmaların geliştirilmesi büyük önem arz etmektedir. Sunulan tez çalışmasında esas alındığı gibi, taşıyıcı verilerin ilk halinin herhangi bir kimsede bulunmamasının sağlanması ve gizli verinin fark edilebilirliğinin çok düşük seviyelerde tutulması gizli haberleşmenin başarımını arttıracaktır.

Tüm lisansüstü çalışmalarım süresince birikimlerini bana aktaran, tezimin başlangıcından bitimine kadar her aşamasında sorunlarımı dinleyen, çalışmalarıma yön veren ve gece gündüz demeden değerli zamanını sorunlarımın çözümüne ayıran tez danışmanım Sayın Prof. Dr. İsmail ERTÜRK'e en içten teşekkürlerimi sunarım. Tez izleme jüri üyesi olan Sayın Doç. Dr. Celal ÇEKEN'e (Kocaeli Üniversitesi) ve Sayın Yrd. Doç. Dr. İbrahim ÖZÇELİK'e (Sakarya Üniversitesi) yardım ve destekleri için teşekkür ederim. Ayrıca çalışmalarım boyunca düşüncelerinden yararlandığım Yrd. Doç. Dr. Feyzi AKAR'a (Deniz Harp Okulu), yardım ve desteklerini gördüğüm değerli arkadaşlarım Alper KARAHAN (Kocaeli Üniversitesi), Tuncay AKBAL ve Cemil ASLAN'a teşekkür ederim.

Yapmış olduğum bu tez çalışmasının temelini teşkil eden yönteme 2009/044 numaralı proje kapsamında destek veren Kocaeli Üniversitesi Bilimsel Araştırma Projeleri Birimi'ne (KOU–BAP) ve 2211–Yurtiçi Doktora Burs Programı kapsamında çalışmalarıma katkıda bulunan TUBİTAK Bilim İnsanı Destekleme Daire Başkanlığı'na (BİDEB) teşekkür ederim.

Beni bugünlerime getiren, her konuda destek veren ve yanımda olan çok değerli annem Güler ve babam Haşim YALMAN'a, yıllardır manevi desteğini esirgemeyen değerli eşim Neslihan YALMAN'a ve geceleri aralıksız uyuyarak akademik çalışmalarımı bölmeyen sevgili oğlum Serdar Ali YALMAN'a çok teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER

c	: Işık hızı (m/s)
E	: Enerji (Joule)
f	: Frekans (Hz)
h	: Planck sabiti (Joule.sn)
L	: Bit derinliği (bit)
m	: Sütun sayısı
n	: Satır sayısı
Q	: Kalite indeksi
r	: Yansıtma
λ	: Dalgaboyu (m)

Kısaltmalar

AES	: Advanced Encryption Standard
ASCII	: American Standard Code for Information Interchange
ASD	: Alt Sınır Değeri
AVI	: Audio Video Interleave
BIQI	: Blind Image Quality Indices
BMP	: Bitmap
BPS	: Bit Per Second
CCD	: Charge Coupled Device
CER	: Constant Embedding Rate
CIF	: Common Interchange Format
CMYK	: Cyan Magenta Yellow Black
DCT	: Discrete Cosine Transform
DES	: Data Encryption Standard
DFT	: Discrete Fourier Transform
DPCM	: Differential Pulse Code Modulation
DPI	: Dot Per Inch
DSS	: Digital Signature Standard
DWT	: Discrete Wavelet Transform
ECC	: Elliptic Curve Cryptography
FPS	: Frame Per Second
HDTV	: High Definition TV
HSI	: Hue Saturation Intensity
HSV	: Histogram based Steganography on Video
HVS	: Human Visual System
ICT	: Irreversible Color Transform
ISDN	: Integrated Services Digital Network
ITU	: International Telecommunication Union

İDS : İnsan Duyu Sistemi
İGS : İnsan Görme Sistemi
JPEG : Joint Photographic Experts Group
LSB : Least Significant Bits
MPEG : Motion Pictures Experts Group
MSE : Mean Square Error
M–SSIM : Mean–Structural Similarity
NTSC : National Television Standards Committee
OSI : Open System Interconnection
PAL : Phase Alternate Line
PD : Parlaklık Değeri
PPI : Pixel Per Inch
PSNR : Peak Signal to Noise Ratio
QAM : Quadrature Amplitude Modulation
QCIF : Quarter CIF
RCT : Reversible Color Transform
RGB : Red Green Blue
RLC : Run Length Coding
RSA : Rivest Shamir Adleman
SECAM : Système Electronique Couleur Avec Mémoire
SIF : Standard Interchange Format
StegVid : Steganography on Video
UQI : Universal Image Quality Index
ÜSD : Üst Sınır Değeri
WIPO : World Intellectual Property Organization
WMV : Windows Media Video
VCR : Video Cassette Recording
VER : Variable Embedding Rate
VF : Varlık Frekansı
VIF : Visual Information Fidelity

SAYISAL GÖRÜNTÜLER İÇİN HİSTOGRAM TEMELLİ VERİ GİZLEME YÖNTEMİ VE UYGULAMA YAZILIMI

Yıldıray YALMAN

Anahtar Kelimeler: Veri Gizleme, İmge Histogram Değişimi, Sayısal Görüntü.

Özet: Yüzyıllardır süregelen bilgi birikiminin geometrik bir dizi gibi artması ile birlikte teknoloji hızla gelişmekte, birbirini etkileyen bu durumlar ise bilgi ve bilginin korunması konularını ön plana çıkarmaktadır. Bilgisayarların artık sayısal ortamlarda daha kolay haberleşebilmeleri olumlu bir gelişme olmakla birlikte, bu durum kullanıcıların evlerini tüm dünyaya açmaları anlamına da gelmektedir. Bu noktada kişisel bilgilerin gizliliğinin sağlanması büyük önem taşımaktadır.

Bu tez çalışmasında özel veya gizli bilgilerin, istenmeyen kişilerce elde edilmesini, değiştirilmesini ya da bozulmasını önlemek amaçlarıyla histogram temelli yeni bir veri gizleme yöntemi (HSV) ve uygulaması (StegVid) sunulmaktadır. Veri gizleme biliminin uygulandığı sayısal ortamların, ihtiva ettikleri gizli veriye ilişkin herhangi bir işaret taşımamaları çok önemlidir. Gömü verisi kapasitesi ve örtü verisinde oluşan bozulma düzeyi ile dengelenen bu hassas durumda, en öncelikli amaç bilginin güvenliğinin sağlanmasıdır. Geliştirilen HSV yöntemi, gömü verilerini gerçek zamanlı sıralı imgelerde (sayısal görüntü) saklamayı hedeflemektedir. Dolayısıyla taşıyıcı ortamın orijinali üçüncü şahıslarda bulunmamakta ve yüksek veri gizleme kapasitesi mümkün olmaktadır. Bununla birlikte taşıyıcı ortamda, görsel veya istatistiksel olarak gizli verinin varlığına işaret eden ve literatürde tanımlanan durumlar ortadan kaldırılmaktadır.

Geleneksel veri gizleme uygulamalarına görüntü histogramlarında tarak etkisi oluşumunu önleyen yeni bir yöntem sunan HSV algoritması ve gerçeklenen StegVid uygulaması, gömü verisi kapasitesini en iyilerken, örtü verisinde meydana gelen bozulma düzeyini son derece düşürmektedir.

DESIGN AND IMPLEMENTATION OF A STEGANOGRAPHY METHOD BASED ON HISTOGRAM MODIFICATION FOR DIGITAL IMAGES

Yıldıray YALMAN

Keywords: Steganography, Image Histogram Modification, Digital Images.

Abstract: Together with the ever increasing improvement of technology, which has led to development of knowledge, the issue of information protection has become vital. Recently, computers have been able to communicate more easily in digital environments and, in this way users open their homes to the world. At this point, to ensure the confidentiality of personal and critical information is of great importance.

In this thesis, to prevent confidential information to be obtained, altered or corrupted by third parties, a new histogram based data hiding method (HSV: **H**istogram based **S**teganography on **V**ideo) and its application (StegVid: **Steg**anography on **Vid**eo) are presented. It is important for the processed digital media (image or video), used for data hiding, not to reflect any sign or trace of about the hidden data. The proposed method is designed to achieve high efficiency and, it well trades off the data embedding capacity and the cover image distortion from the original. The proposed HSV aims to hide embedded data in real–time videos also. As a result, both the third parties can not have the original cover media for steganalysis and high data hiding capacity can be easily achievable. In addition to these advantages, HSV does neither cause any visual distortion nor statistical negation on the cover media described in the literature.

The HSV and its application software StegVid offer a new data hiding approach based on image histogram modification canceling the combing effect. The HSV enables highly optimized hidden data embedding capacity while minimizing the visual or statistical distortion on the cover media.

1. GİRİŞ

Veri gizleme üzerine yapılan çalışmalar, telif hakları ve bilgi güvenliği uygulamaları gibi güncel gereksinimler ile gün geçtikçe yaygın bir öneme sahip olmaktadır. İnternet ve iç ağ teknolojilerinin gelişmesi ve hızla yayılması ile her evin içerisinde dünyaya açılan bir kapı bulunmakta ve mesafeler hızla ortadan kalkmaktadır. Bu muazzam ve kontrol edilemez büyüklükteki iletişim ortamında güvenliğin tam anlamıyla sağlanması da neredeyse imkânsızdır. Özellikle bireysel iletişim hayatının mahremiyetini korumak, bireyler arası haberleşme güvenliğini sağlamak günümüzde önemli ve çok popüler bir konu haline gelmiştir. Bu nedenle veri gizleme tekniklerinin önemi iletişim sistemleri içerisinde giderek artmaktadır. Gizliliğin kritik bir gereksinim olduğu uygulamalarda; gizli bilgilerin, üçüncü kişilerin eline geçmeden ilgili hedefe ulaştırılması amaçlanır ve bu amaçla yöntemler geliştirilir.

Verilerin gizlenmesinde kapasite, ataklara karşı dayanıklılık, güvenlik ile tez çalışmasının başlatılma sebebini de oluşturan sezilemezlik (inperceptibility) ön plana çıkan ana unsurlardır. Günümüze kadar veri gizleme alanında birçok çalışma/araştırma gerçekleştirilmiştir. Aşağıdaki alt bölümde bu çalışmalardan birkaçı kısaca özetlenmektedir.

1.1. Literatürde Yapılan Çalışmaların Özetleri

Jung ve Yoo (2009) geliştirdikleri yöntemde ilk olarak verinin gizleneceği imgenin çözünürlük değerini ara değerleme yaparak arttırmışlardır. İmgenin orijinal piksel değerlerinde değişiklik yapılmadan eklenen yeni sayısal değerlere veriler gizlenmiş ve gömü verisinin elde edilmesinin ardından taşıyıcı imgenin ilk haline dönmesi sağlanmıştır. Bu teknik taşıyıcı imgenin herhangi bir kayba uğramadan elde edilmesini sağlasa da, imge boyutunu dört katına çıkardıktan sonra veri gizleme işlemi yaptığından hem işlem yükü arttırılmakta hem de imgenin görüntü kalitesi bozulduktan sonra veri gizleme işlemi yapılmaktadır. Bu durum uygulanan yöntemin

olumsuz yönünü teşkil etmektedir. Tepe Sinyal Gürültü Oranı (Peak Signal to Noise Ratio: PSNR) 35 dB değerinin üzerinde olsa da yapılan çalışmada histogram görüntülerine ilişkin bir değerlendirme yapılmamıştır. Bu yöntem bit uzayında işlemleri gerçekleştirmesi açısından sunulan tez çalışması ile benzerlik gösterirken, algılanabilirlik ölçütleri (UQI, M–SSIM vb.) açısından daha düşük değerlere sahiptir.

Huang ve Fang (2008) yapmış oldukları çalışmada imge histogramını kullanarak veri gizleme işlemini gerçekleştirmişlerdir. İlgili yöntem imgedeki bozulmanın göz ile algılanamamasını sağlasa da, histogram açısından durum değişmektedir. Histogram içerisinde varlık frekansı en yüksek olan parlaklık değeri kullanılarak gerçeklenen veri gizleme işlemi, gözle algılanabilir bir değişime sebep olmaktadır. Tez çalışmasının temel motivasyonlarından birini oluşturan histogram üzerinde algılanabilir bozucu etki oluşturmama ilkesi bu çalışmada söz konusu değildir. Aynı zamanda yazarlar geliştirmiş oldukları yönteme ilişkin sayısal başarım değerleri açısından detaylı değerlendirme yapmamışlardır.

Ni ve diğ. (2008) sıkıştırılmış imgeler üzerine uygulanabilen ve geri dönüştürülebilir bir yöntem önermişlerdir. Histogram bilgisinin bir çember etrafında dizilimini esas alarak veri gizleme işlemini başlatan bu yöntemde PSNR değerleri kabul edilebilir seviyelerde olsa da gömü verisi kapasitesi oldukça düşüktür. Başarım analizleri arasında ise histogram görünümlerine ilişkin herhangi bir karşılaştırma yapılmamıştır.

Chrysochos ve diğ. (2007) imge histogramını temel alan bir veri gizleme yöntemi ele almışlardır. Bu yöntemde imgelerde ve imge histogramlarında değişimler gözle algılanamamaktadır ancak, tez çalışmasında sunulan sonuçlara oranla daha düşük gömü verisi kapasitesine ve daha düşük PSNR değerlerine sahiptir.

Bhatnagar ve Raman (2008) ataklara dayanıklı bir damgalama tekniği önermişlerdir. Önerilen teknikte gömü verilerinin elde edilme sürecinde referans imgeye ihtiyaç duyulmaktadır. Bu durum yöntemin en büyük eksikliği olarak görülmektedir. Çünkü referans imgeye ulaşmak gömü verisinin elde edilmesi sürecinde her zaman mümkün

olmayabilir. Bununla birlikte çalışmada görsel analizlere yer verilirken sayısal başarım değerlerine yer verilmemektedir.

Akar ve Varol (2004) önerdikleri veri gizleme yönteminde literatürde sunulan birçok çalışmadan daha fazla gömü verisi kapasitesi sunan RGB ağırlık tabanlı kodlama tekniğini geliştirmişlerdir. PSNR değerleri açısından da oldukça iyi sonuçlar veren bu yöntem görsel analizde de başarılı olsa da, imge histogramları açısından oldukça olumsuz sonuçlar vermekte, doğal imgelerin histogramlarında gerçekleşmesi neredeyse imkânsız olan tarak etkisine sebep olmaktadır.

Hongmei ve diğ. (2003) askeri ve sağlık alanlarında kullanılmak üzere geliştirdikleri yöntemde, belirlenen renk çiftlerini esas alarak veri gizleme işlemi gerçekleştirmektedir. Yapılan çalışmada sadece gömü verisi kapasitesi açısından değerlendirme yapılmış olması, sayısal başarım ölçütlerine yer verilmemesi olumsuz bir sonuç teşkil etmektedir.

1.2. Tez Çalışmasının Amacı Ve Başlatılma Sebebi

Her ne kadar bilgi güvenliği kavramı askeri amaçlarla ortaya çıksa da, bilgisayar ve internetin olduğu hemen her alanda bireylerin kişisel bilgilerinin güvenliğine ilişkin sorunlar gündemden düşmeyen bir konudur. Bu noktada öne çıkan, bilgilerin gizlenme şeklidir. Kişisel/özel bilgilere ulaşması istenmeyen kişilerin, yapacakları araştırmalar sonucunda söz konusu bilgilere ulaşabilme zorluğu, oluşturulan yöntemin başarısına ilişkin önemli bir ölçüttür. Sunulan tez çalışmasının da en önemli başlatılma sebebini oluşturan, verilerin taşıyıcı bir ortamda fark edilmeyecek şekilde saklanması amacıyla yeni yöntemler geliştirilmektedir. Bu yöntemler genellikle gömü verisi kapasitesine ve görsel bozulmaların en aza indirgenmesine odaklanmıştır. Ancak bununla birlikte sunulan tez çalışmasının detaylarında da vurgulanan sayısal başarım analizleri, histogram değişimleri ve taşıyıcının orijinal halinin başkalarında bulunma durumu da dikkate alınmalıdır.

Günümüzde internet iletişim hızının giderek geliştiği ve bilgisayarların depolama kapasitelerinin arttığı göz önünde bulundurulduğunda görsel kalitesinden hiçbir ödün

verilmeyen ham imge ve hareketli görüntü kayıtlarının (video) depolama ve internet ortamında kullanımı eskiye oranla daha caziptir. Gömü verisi kapasitesi açısından da oldukça olumlu sonuçlar veren bu ortamlar (özellikle videolar) veri gizleme algoritmaları için çok uygun kaynaklardır.

Özetle, bu tez çalışmasının üç ana hedefi bulunmaktadır;

- Görsel ve sayısal değerlendirmeler sonucunda şüphe uyandırmayacak sonuçlar veren histogram temelli yeni bir veri gizleme yöntemi (HSV) geliştirmek,
- İlgili yöntemi örtü verisi olarak gerçek zamanlı hareketli görüntü kayıtlarının kullanıldığı bir uygulama yazılımı (StegVid) ile gerçeklemek ve
- Literatürdeki eşleniklerine kıyasla örtü verisinde oluşan bozulma düzeyini ifade eden istatistiksel başarımı arttırırken, daha yüksek gömü verisi kapasitesi elde etmektir.

1.3. Tez Çalışmasının Katkıları

Sunulan tez çalışmasında gerçek zamanlı hareketli görüntü kayıtları için yeni bir veri gizleme yöntemi (HSV) önerilmektedir. Bu yöntem, görsel olarak taşıyıcı imgeler üzerinde eşleniklerine oranla daha yüksek gömü verisi kapasitesi sağladığı gibi, istatistiksel açıdan da sezilemezlik ilkesine uygun sonuçlar vermektedir. HSV ile bilime ve teknolojiye iki temel katkı sağlanmıştır;

- Klasik birçok yöntemin taşıyıcı imgelere veri gizlemesinin ardından histogramlarda oluşturduğu bozucu etki (tarak etkisi) sunulan tez çalışmasında önerilen veri gizleme yöntemi HSV uygulandığında ortaya çıkmamaktadır. Bu sayede histogramın görsel analizinin yapılması sonucunda gömü verisinin varlığından şüphelenilmemektedir.
- Gömü verisinin herhangi bir örneğinin kodlamayı yapan kullanıcı da dâhil hiç kimsede olmamasını sağlamak amacıyla, gerçek zamanlı hareketli görüntüler kullanılmakta, bu sayede orijinal veri ile karşılaştırma yapılamaması sağlanarak algılanamazlık ilkesi en üst seviyeye taşınmakta ve geliştirilen uygulama yazılımı (StegVid) ile de bu durum doğrulanmaktadır.

Tez çalışmasının yukarıda ifade edilen ana katkılarının yanı sıra bazı ek özellikleri de bulunmaktadır. Bunlar aşağıda maddeler halinde sıralanmıştır;

- Geliştirilen algoritma imge histogramlarını kullandığından gömü verisi kapasitesini arttırmak için, imgeler küçük parçalara bölündükten sonra her bir parçanın histogramına veri gizlenebilmekte yani gömü verisi kapasitesine ilişkin esneklik sağlanmaktadır.
- İmgedeki piksellerin ya da rasgele bölümlerin yer değiştirmesi sonucunda histogram değişmeyeceğinden gömü verisi kaybolmayacak ya da gömü verisinin dizilişi bozulmayacaktır. Bu da geliştirilen HSV yönteminin, histogramı değiştirmeyen geometrik ataklara karşı dayanıklı olduğunu göstermektedir.
- Tarak etkisinin oluşmasını engellemek için imge histogramının kullanıldığı bu tez çalışmasından hareketle bir imgede gömü verisinin varlığına ilişkin şüphelerin, tarak etkisi ile doğru orantılı olarak artacağı gösterilmektedir.
- Gömü verisinin elde edilmesi sürecinde örtü verisine ihtiyaç duyulmamakta ve gömülü veri kullanılarak gizli veriler elde edilmektedir.
- Geliştirilen yöntem sadece RGB imgelere değil, gri tonlu imgelere de uygulanabilmektedir.

1.4. Tez Düzeni

Bölüm 2'de, Veri gizleme başlığı altında incelenen ve günümüzde sıklıkla kullanılan şifreleme, damgalama ve steganografi bilimleri ile uygulamaları detaylı şekilde açıklanmaktadır.

Bölüm 3'te, Sayısal görüntünün temellerini oluşturan piksel, imge, çözünürlük gibi kavramlar açıklanarak bu kavramlar ile ilgili sayısal işlemlere ve renk modellerine yer verilmektedir.

Bölüm 4'te, Sayısal görüntüler için geliştirilen histogram temelli veri gizleme yönteminin (HSV) veri gizleme ve gömülü gizli veriyi elde etme işlemlerine ilişkin adımlar ve akış şemaları verilmekte, uygulama yazılımı StegVid sürümleri tanıtılmaktadır.

Bölüm 5’te, StegVid kullanımı sonucunda elde edilen deneysel sonuçlara ilişkin detaylı başarım analizleri sunulmaktadır.

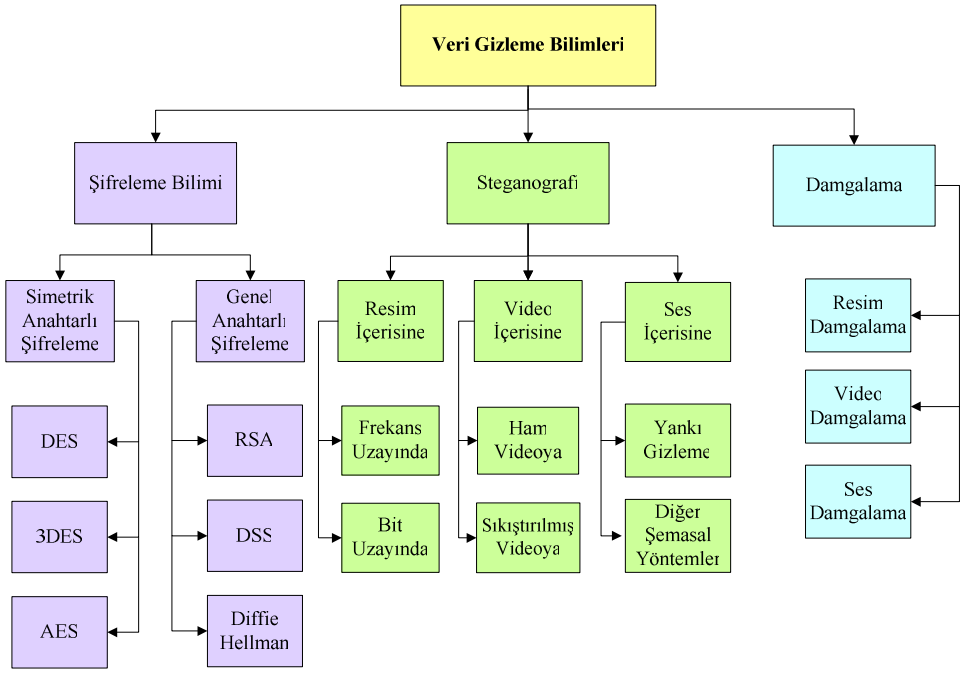
Geliştirilen HSV yönteminin ve StegVid uygulamasının temel özellikleri, bilime ve teknolojiye sunmuş olduğu katkılar, sonuçlar ve değerlendirmeler Bölüm 6’da ifade edilmektedir. Bu bölümde ayrıca, HSV’nin geliştirilmesine ve uygulanmasına yönelik öneriler de yer almaktadır.

2. VERİ GİZLEME BİLİMİ

2.1. Giriş

Bilgisayar ve internet teknolojisindeki gelişmelere paralel olarak, bilgi paylaşım kolaylığı, hızlı işlenebilirlik ve büyük boyutlu saklanabilirlik gibi özelliklere sahip sayısal ortamlarda da önemli gelişmeler olmuştur. Bu sayede insanlar sadece yazılı metinleri paylaşmakla sınırlı kalmayıp, bir ortama ait resimleri, kaydedilmiş bir ses kaydını veya yapılan önemli bir toplantının görüntülerini de paylaşabilme imkânına sahip olmuşlardır.

Teknolojinin bilgi paylaşımında sağlamış olduğu bu kolaylıklar karşısında beraberinde getirdiği en önemli tehdit haberleşmede mahremiyetin sağlanamamasıdır. Örneğin üçüncü kişilerin ulaşmasının istenmediği bir video dosyasına ait çerçeveler internet üzerinden farklı yollardan alıcıya gönderilerek haberleşme sağlanabilir (Karlsson ve diğ., 2005). Ancak alıcıya giden her bir çerçevenin güvenliğinin de sağlanması önemli bir sorundur (Yılmaz, 2003). Bu nedenle haberleşmede gizliliği sağlamak için yeni çalışmalar yapılmaktadır. Veri gizleme olarak bilinen bu çalışmalarda amaç; haberleşme esnasında yetkisiz veya izinsiz kişilerin haberleşme materyallerine ulaşmalarını engellemek ya da ulaşılan materyalleri yetkisiz kişilerce anlaşılmayacak bir forma dönüştürmektir. Bu bölümde literatürde veri gizleme başlığı altında yer alan şifreleme (kriptoloji), damgalama (watermarking) ve steganografi üzerinde durularak bilgi güvenliğindeki rolleri, birbirlerine olan üstünlükleri ve farklılıkları vurgulanmaktadır (Şekil 2.1). Bununla birlikte tez çalışmasının temelini teşkil eden hareketli görüntü kayıtlarına steganografi yönteminin uygulanma amacı vurgulanmaktadır.

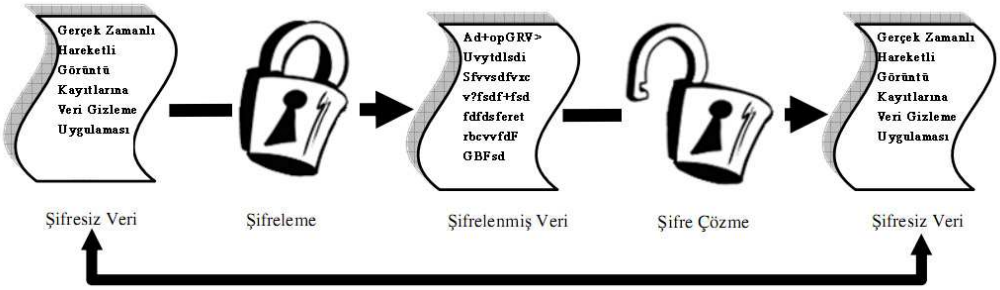


Şekil 2.1: Veri gizleme bilimleri ve çeşitleri.

2.2. Şifreleme

Şifreleme (Cryptography) kelimesi gizli yazı anlamına gelen, “secret (crypto–)” ve “writing (–graphy)” kelimelerinden türetilmiştir. Şifreleme, gizli ve yüksek öneme sahip verilerin çeşitli mantıksal/matematiksel ifadeler kullanılarak anlaşılamamasını sağlayan bir bilim dalıdır. Başka bir ifade ile haberleşen iki veya daha fazla tarafın bilgi alış verişini emniyetli olarak yapmasını sağlayan ve gizli ya da özel bilgiyi istenmeyen kişilerin anlayamayacağı hale getirerek korumayı esas alan, temeli matematiksel yöntemlere dayalı tekniklerin ve uygulamaların bütünüdür (Yalman ve Ertürk, 2008). Simetrik anahtarlı (gizli anahtar, secret key) ve asimetrik anahtarlı (açık anahtar, public key) olmak üzere iki temel şifreleme yöntemi mevcuttur. Simetrik anahtarlı şifreleme tekniğiyle geliştirilen algoritmaların güvenliği anahtar uzunluğuna bağlı olarak değişir. Bu algoritmalar oldukça hızlı çalışırlar. Asimetrik anahtarlı şifreleme tekniğiyle geliştirilen algoritmalar ise şifreleme ve şifre çözme için birbiriyle matematiksel olarak ilişkili iki farklı anahtar kullandıklarından, güvenli fakat özellikle büyük veri yığınları için çok yavaştırlar (Menezes ve diğ., 1996, Akbal, 2008, Bandırmalı, 2010).

Özel bir yöntem kullanmadan okunabilen ve anlaşılabilen veriye şifresiz veri (plaintext, cleartext), şifresiz verinin herhangi bir şekilde gizlenmesini sağlayan yönteme şifreleme (encryption), şifresiz verinin şifrelenmesiyle oluşan ve okunduğunda anlaşılamayan ifadelere ise şifrelenmiş veri (ciphertext) adı verilmektedir. Şifreli verinin orijinal şifresiz veri haline dönme işlemi ise şifre çözme (decryption) olarak adlandırılmaktadır (Şekil 2.2).



Şekil 2.2: Şifreleme ve şifre çözme blok şeması.

Şifreleme ile hassas verinin güvenli bir şekilde saklanması ya da güvenli olmayan bir ağda iletilen verinin planlanan alıcılar dışında herhangi bir alıcı tarafından anlaşılamaması sağlanır (Meka, 2007). Şifrelenmiş verinin güvenliği, büyük oranda şifreleme algoritmasının dayanıklılığı ve anahtarın gizliliğine bağlıdır (Bandırmalı, 2010).

Şifreleme yöntemlerinin başarımı şu ana ölçütlere göre belirlenir:

- Kırılma süresinin uzunluğu,
- Şifreleme/şifre çözme işlemlerinde harcanan zaman (zaman karmaşıklığı),
- Şifreleme/şifre çözme işlemlerinde ihtiyaç duyulan bellek miktarı (bellek karmaşıklığı),
- Kullanılan algoritmaya dayalı şifreleme uygulamalarının esnekliği,
- Uygulamaların dağıtımındaki kolaylık ya da algoritmaların standart hale getirilebilmesi ve
- Algoritmanın kurulacak sisteme uygunluğu (Tektaş ve diğ., 2003).

Simetrik anahtarlı şifrelemede, şifreleme ve şifre çözme işleminde kullanılan anahtarlar aynıdır. Bu anahtar sadece orijinal metine ulaşması istenilen kişilere verilir. Haberleşecek kişiler önceden anahtarı belirlerler. Simetrik şifrelemenin güvenliği anahtarın güvenliğine bağlı olduğundan, anahtarın gizli tutulması çok önemlidir (DES, 3DES ve AES algoritmaları).

Genel anahtarlı şifreleme asimetrik şifreleme olarak da bilinir. Simetrik anahtarlı şifrelemeye göre çok yavaş olmasına karşın, simetrik şifrelemedeki şifreleme ve şifre çözme anahtarı dağıtımı problemine çözüm getirmektedir (Schneier, 1996, Verheul ve diğ., 1997, Yerlikaya ve diğ., 1995). Asimetrik şifrelemede iki adet anahtar oluşturulur. Bunlar orijinal bilginin şifrelenmesinde kullanılan genel anahtar ve şifre çözme işleminde kullanılan özel anahtarlardır. Genel anahtar olarak belirtilen anahtar herkese açıktır ve bu durumun herhangi bir sakıncası yoktur (De Santis ve Spagnolo, 2006). Çünkü genel anahtarla sadece bilgiler şifrelenir ve bu şifreli bilgiler sadece genel anahtar kullanılarak üretilmiş özel anahtar kullanılarak çözülebilir. Bu nedenle özel anahtarın gizliliği asimetrik şifrelemede büyük önem taşımaktadır (RSA, Diffie–Hellman, DSS, ECC algoritmaları).

Telif haklarının korunması veya yetkisiz kullanıcıların izlemesini engellemek amacıyla video dosyalarına ait çerçeveler de ayrı ayrı şifrelenebilmektedir (Lian ve diğ., 2007). Bu noktada gizli haberleşme amacıyla simetrik ya da asimetrik şifrelemenin kullanılmasına bağlı olmaksızın, güvenilirlik sağlansa da mesajın gizliliği sağlanamamaktadır. Şifreleme uygulamalarında bilgi, sadece gönderen ve alanın anlayabileceği şekilde şifrelenir. Üçüncü kişilerin şifrelenmiş bilgi bloğunu elde etmeleri halinde anlamsız gibi görünen bu bloktan şüphelenmeleri ihtimali oldukça yüksektir (Yalman, 2007). Çünkü mesaj anlamsızda olsa elde edilmiştir. Bu sebeple araştırmacılar şüphe uyandırmayan diğer teknikler olan damgalama ve steganografi bilimine yönelmişlerdir.

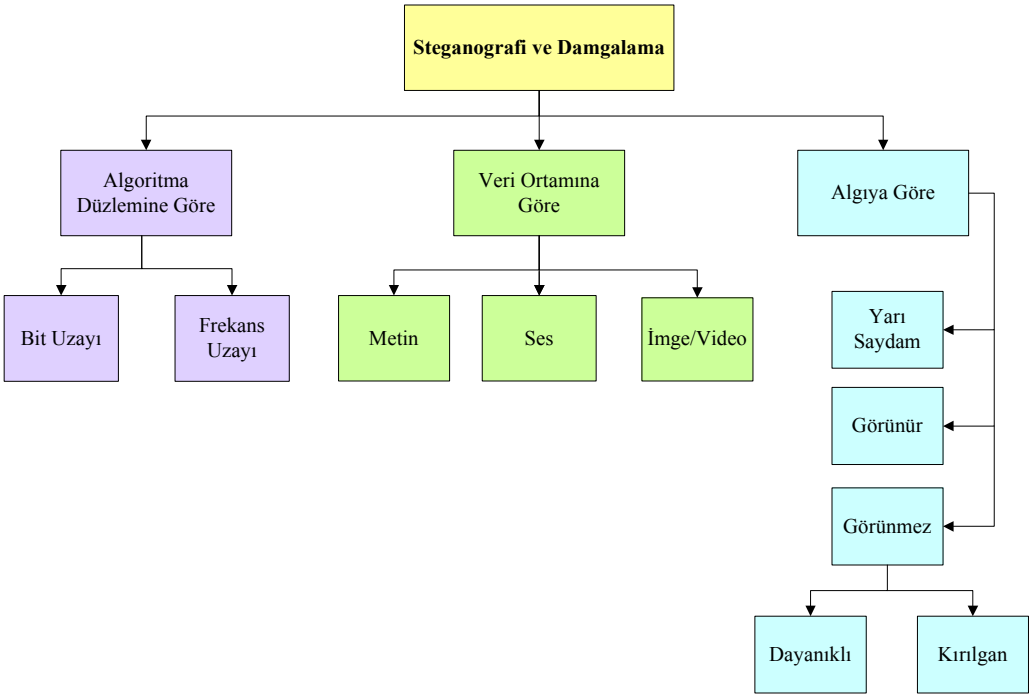
2.3. Sayısal Damgalama

Veri gizleme tekniklerinin ticari kullanımı sayısal “filigran” kavramının gelişmesine sebep olmuştur. Özellikle internet aracılığı ile paylaşılan sayısal çoklu ortam

verilerinin korunması problemi ile ilgili çalışmalar damgalama araştırmalarına konu olmuştur. Sahiplik bilgisi ve telif hakkı gibi kimi bilgilerin ilgili ortamlar (media) içerisine yerleştirilmesi yönünde yoğun çalışmalar yapılmıştır. Damgalama tekniklerinde en önemli amaç herkes tarafından bilinen, popüler bir sayısal medyanın kanunsuz yollarla çoğaltılmasını ya da dağıtılmasını önlemek yani eser sahibinin telif hakkını korumaktır (Cox ve diğ., 2000). Aslında, orijinal bir eserin korunmasını önlemek için geliştirilen koruma yöntemleri daha da eskilere dayanır. Kâğıt banknotlar üzerinde yer alan ve ışığa tutulduğunda görülen filigranlar, kitapların kapaklarında bulunan hologramlar bunlara örnektir. Günümüzdeki anlamıyla damgalama 1950'li yıllarda bir müzik şirketinin müzik kayıtlarına sahiplik bilgisini yerleştirmesi ile ortaya çıkmıştır. 1990'ların başında Tanaka ve diğ. (1990) faks gibi ikili imgelerin korunması (imge damgalama) kavramını ortaya atmışlardır. 1993 yılında Tirkel ve arkadaşları gerçekleştirdikleri veri gizleme tekniğine, daha sonraları "watermark" olarak birleştirilen "water mark" ismini vermişlerdir (Hartung ve Kutter, 1999).

Damgalama tekniklerinin uygulandığı ortamlar ataklara açık yapıda olduklarından, gömü verisinin örtü verisinden ayrıştırılamamasının sağlanması birinci öncelikli konu olarak araştırmacıların karşısına çıkmaktadır. Özellikle müzik dosyaları için telif haklarının korunması amacıyla ses damgalama (audio watermarking) adı verilen çalışmalar genel olarak gömülü gizli verilerin sezilemezliği üzerine yoğunlaşmıştır. Dünya çapında telif haklarının korunması ve düzenlenmesi ile ilgili çalışmalar yapan ve hükümetler üstü bir kuruluş olan WIPO (World Intellectual Property Organization) sayısal veri gizleme sistemlerinin yasal alanlarıyla ilgili çalışmalar yapmaktadır (Delaigle, 2000).

Genel olarak bakıldığında steganografi ve damgalama birbiri ile neredeyse aynı yapıya sahip iki tekniktir. Damgalamayı steganografiden ayıran en belirgin özellik popüler medya üzerinde uygulanmasıdır. Şekil 2.1'de sınıflandırması yapılmış olan veri gizleme bilimlerinden steganografi ve damgalamanın uygulanma şekilleri Şekil 2.3'te detaylandırılmaktadır.



Şekil 2.3: Steganografi ve Damgalama bilimlerinin uygulanma şekillerine göre sınıflandırılması.

Görünür sayısal damgalama uygulamalarında, sayısal medyanın içerisine yerleştirilen damga İnsan Görme Sistemi (İGS) tarafından rahatça algılanabilir. Ticari amaçla üretilmiş bir ürünün hangi kuruma ait olduğunu gösteren damgalar ve televizyon kanallarının yayınlarında kullandıkları ekran logoları görülebilir sayısal damgalama uygulamalarına verilebilecek örneklerdir (Echizen ve diğ. 2006).

Görünmez sayısal damgalama uygulamalarında ise, damga bilgisi İGS veya İnsan Duyma Sistemi (İDS) tarafından algılanamaz (Zhang ve Wang, 2005). Piyasaya yeni çıkarılmış olan bir sinema filminin DVD'sinin veya müzik CD'sinin kopyalamalara karşı korumak amacıyla görülemez sayısal damgalama kullanılır.

Sayısal damgalama ile korunmuş sayısal medya parlaklık ve karşıtlık (contrast) ayarlarının değiştirilmesi, özel filtrelerin kullanılması, kâğıda baskı veya tarama gibi saldırılara karşı korunabilmektedir. Ancak StirMark ve UnZign gibi damgalama teknolojisinden hemen sonra ortaya çıkan bazı programlar sayısal damgayı kaldırabilmekte veya etkisiz hale getirebilmektedirler. Asıl amaçları geliştirilen

damgalama tekniklerinin performans değerlendirmelerini yapmak olan bu programlar aynı zamanda sayısal damgayı da yok ederek saldırı amaçlı programlar haline de gelebilmektedirler.

Sayısal damgalamanın sağlaması gereken bazı önemli gereksinimler vardır. Bu gereksinimler sayısal damgalamanın kullanılacağı uygulamaya göre değişiklik gösterebilir (Barni ve Bartolini, 2004) ve genel olarak aşağıdaki gibi sıralanabilirler:

- Dayanıklılık: Sayısal damga, kasıtlı saldırılara karşı korunan bilgilerin zarar görmesini engellemelidir.
- Algılanamazlık: Özellikle görülemez sayısal damgalama uygulamalarında, lisanssız veya izinsiz kullanıcıların görsel inceleme sonucunda damgayı görememeleri gerekmektedir.
- Güvenlik: Sayısal damga yetkisiz veya kötü niyetli kişiler tarafından yapılacak sayısal incelemelerde fark edilememelidir.
- Hızlı gizleme ve geri elde etme: Özellikle internet üzerinden paylaşılan sayısal medyanın damgalama işleminin hızlı olması önemlidir.
- Orijinal dosyaya ihtiyaç duymama: Bazı uygulamalarda taşıyıcı medyanın orijinali olmadan sayısal damganın geri elde edilmesi gerekmektedir. Aynı zamanda bu durum güvenliği de artıran bir unsurdur.

Hareketsiz görüntüler üzerinde yapılan ilk sayısal damgalama çalışmalarında en düşük değerlikli bit (LSB: Least Significant Bit) değiştirme yöntemi kullanılmıştır. Örneğin gizli veri en düşük değerlikli iki bit içerisine gömülmüştür (Schyndel ve diğ. 1994). Bir başka çalışmada ise gizli veri geometrik bir şekil olarak sayısal görüntünün algılanamayan parlaklık bilgisine gömülmüştür (Caronni, 1995).

Fakat bu çalışmalar saldırılara (attack) karşı yeterli dayanıklılığı (robustness) sağlayamamaktadır. Daha dayanıklı bir yöntem olarak sayısal damganın alçak geçiren bir filtre ile desteklenmesi literatürde önerilen ve genel kabul gören bir yaklaşımdır (Braudaway, 1997).

Araştırmacılar daha dayanıklı damgalama yöntemleri geliştirmek için ayrık kosinüs (DCT: Discrete Cosine Transform) (Ahmed ve diğ., 1974), ayrık dalgacık (DWT: Discrete Wavelet Transform) (Rioul ve Duhamel, 1992) ve ayrık fourier (DFT: Discrete Fourier Transform) (Brigham, 1974) dönüşümlerinin kullanımını önermişlerdir. Cox ve diğ. (1997) çalışmalarında, bir damgalama yönteminin saldırılara karşı dayanıklı olması için, damgayı resmin en önemli algılanabilir bölgelerinin DCT katsayılarına gizlemeyi önermişlerdir. Saldırıların taşıyıcı resme hasar vermeye yönelik değil, damganın silinmesine yönelik olması bu teoriyi desteklemektedir. Fakat bu yöntemin başarısı algılanabilirliğin en alt seviyede tutulmasına bağlıdır.

Xia ve diğ. (1997) DWT dönüşümüne göre damgalama yöntemi geliştirmişlerdir. Bu yöntemde damga, Gaussian gürültüsü olarak modellendikten sonra resmin orta ve yüksek frekans bileşenlerine gömülmektedir. Bu tekniğin DCT tekniğinden daha dayanıklı olduğu görülmüştür.

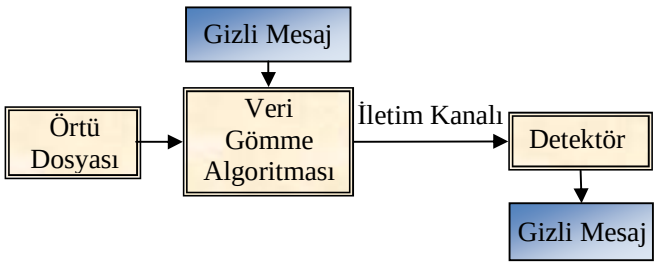
2.4. Steganografi

Günümüzde hızla gelişen internet ve diğer sayısal ağ teknolojileri; çok çeşitli sayısal medyanın kalitesini bozmadan, yüksek kalitede paylaşabilme imkânı sunar. Bu durumun bireylere çok büyük kolaylık sağladığı söylenebilir. Fakat bu muazzam büyüklükteki sanal dünya güvenlik problemleri sebebiyle birçok sorunu da beraberinde getirmiştir. Örneğin sayısal medyanın yasadışı ve korsan dağıtımı büyük bir ekonomik kayba yol açmaktadır (Alattar ve diğ., 2003).

Bir diğer sorun ise, bireyler arasındaki haberleşme mahremiyetinin ihlal edilmesidir. Gerek ekonomik, gerekse güvenlik açısından meydana gelen bu tür olumsuz gelişmeler sayısal medyanın korunması ve güvenli haberleşmenin gerekliliğini ortaya çıkarmıştır (Rabah, 2004). Özellikle terörist saldırılarına ait eylem detaylarının ve planların taşıyıcı sayısal imgelere gömülerek alıcılara ulaştırıldığı iddiaları, 2000'li yıllarda steganografi çalışmalarına hız verilmesine sebep olmuştur.

Steganografi iki parçadan oluşan Yunanca bir kelimedir. “Steganos” örtülü/gizli, “graphy” ise yazım/çizim anlamına gelmektedir. Modern steganografi teknik olarak, bir veriyi ya da mesajı başka bir nesnenin içerisine gizli biçimde yerleştirmeyi esas almaktadır (Johnson ve Jajodia, 1998). Öyle ki, sadece belirlenen alıcı, kendisine iletilmek istenen veriyi ya da mesajı nesneden seçebilmekte ve diğer gözlemcilerin o nesnenin içindeki mesajın varlığından haberleri olmamaktadır (Yalman, 2007). Güvenliğin arttırılması ihtiyacı duyulduğunda, gizli veri ayrıca şifrelenerek arttırılmış koruma sağlanabilir. Bir nesnenin içerisine herhangi bir verinin gizlenmesi olarak da tanımlanan steganografi (Petitcolas ve diğ., 1999); haberleşmede, gizleme bilimi ve sanatı olarak adlandırılır (Provos ve Honeyman, 2003). Kullanım alanındaki esneklik sayesinde mobil sistemlerde de uygulanabilen steganografide asıl amaç gizli bir mesajı hiç kimsenin haberi olmadan kuşku uyandırmayacak şekilde bir başkasına göndermektir (Papapanagiotou ve diğ., 2005, Shahreza ve Shahreza, 2007).

Şekil 2.4’te genel olarak bir veri gizleme işleminin blok diyagramı gösterilmektedir. Diyagrama göre, örtü dosyası ve gizli mesaj bir veri gizleme algoritmasına uygulanır ve elde edilen örtülü dosya bir haberleşme kanalından iletilir. Örtülü dosyayı alan taraf gömülü gizli veriyi elde etme algoritmasını bu dosyaya uygulayarak gizli mesajı elde eder.



Şekil 2.4: Veri gizleme ve gömülü gizli verinin elde edilme şeması.

Örtü dosyası içerisine bir mesaj gizlendikten sonra elde edilen gizli veri içeren yeni haline örtülü dosya ya da stego nesnesi denir. Örneğin, bir yazı dosyasının (covertext) içerisine gizli bir işaret veya bilgi eklendiğinde elde edilen yeni dosya stego–metin (stegotext), veya bir resim dosyası içerisine (cover–image) gizli bir

işaret veya bilgi eklendiğinde elde edilen yeni dosya da stego–imge (stego–image) olarak adlandırılır. Bu terminoloji birinci uluslararası bilgi gizleme seminerinde kabul edilmiştir (Anderson, 1996, Pfitzmann, 1996). Steganografiye ilişkin genel terimler ve tanımlar aşağıda maddeler halinde verilmektedir.

- Örtü Dosyası (Cover–File): İçerisine gizli verinin gömüleceği dosyadır. Bu dosya resim, video veya ses dosyası olabilir.
- Gömü Dosyası (Stego): Gizli veri bloğudur (resim, video, ses, metin vb).
- Gömülü/Örtülü Dosya (Stego–File): Gizli veriye sahip dosyadır (resim, video, ses vb).
- Gömü Anahtarı (Stego–Key): Veri gizleme işlemi sırasında şifrelemeden yararlanıldığı durumlarda kullanılan güvenlik anahtarıdır.
- Steganaliz (Steganalysis): Gizli verinin elde edilmesini sağlamak için yöntem ve teknikler geliştiren bilim dalıdır.

Düzyazı (plaintext), şifreliyazı (ciphertext), resim veya bit dizisi içerisine gömülmüş herhangi bir bilgi ‘gizli veri’ ya da ‘stego’ olabilir. Örtü dosyası ve gizli veri birlikte örtülü dosyayı oluştururlar. Eğer daha fazla güvenlik istenirse bir şifreleme tekniği kullanılarak güvenlik arttırılabilir.

Steganografik tekniklerin başarılı olabilmesi için sağlanması gereken üç önemli gereksinim vardır. Bunlar; gizli haberleşmenin güvenliği, veri gizleme kapasitesi ve kasıtlı veya kasıtsız olarak yapılan saldırılara karşı dayanıklılık olarak sıralanabilir.

- Güvenlik: Bir veri gizleme tekniğinde, gizli veriyi elde etmek için haberleşme kanalını izleyen kötü niyetli kişilerin algısal ve istatistiksel anlamda dikkatlerinin çekilmemesi en önemli güvenlik gereğidir. Güvenli bir sırörtme tekniğinde kötü niyetli kişiler gizli veriye ulaşamamalıdır.
- Kapasite: Veri gizleme tekniklerinde asıl amaç gizli haberleşme olduğu için gizli veri kapasitesinin yüksek olması arzulanır. Fakat gizli veri kapasitesinin artması doğrudan güvenlik zaafiyetine neden olmaktadır. Gizli veri kapasitesi ve güvenlik birbirleriyle ters orantılı olan ve araştırmacıların üzerinde yoğunlaştığı iki önemli parametredir (Marvel ve diğ., 1998).

- Dayanıklılık: Damgalamada olduğu gibi, steganografi tekniklerinin saldırılara karşı dayanıklılık sağlaması çok önem teşkil eden bir parametre değildir. Çünkü gizli haberleşme sırasında kullanılan örtü dosyası herkes tarafından bilinen bir dosya değildir. Fakat örtü dosyası JPEG kodlama yöntemi ile oluşturulmuş ise bu durumda veri gizleme tekniğinin saldırılara karşı dayanıklı olması gerekecektir (Wang ve Wang, 2004).

2.4.1. Steganogafinin tarihçesi

Eski Yunan'da M.Ö. 5. yüzyılda Susa kralı Darius tarafından göz hapsine alınan Histiaeus, Miletus'daki oğlu Aristagoras'a gizli bir mesaj göndermek için kölelerinden birinin saçlarını kazıtır ve mesajını dövme şeklinde kölenin kafa derisine işletir. Kölenin saçları yeterince uzadığında oğlunun yanına gönderir. Kölenin saçlarının kazınması ile Aristagoras mesajı alır. Tarihçi Herodot'un verdiği bu bilgi gizli yazma sanatı steganografinin ilk olarak nerede, nasıl ve kimler tarafından kullanıldığını açıklamaktadır.

Eski Romalılar satırların arasına gözle görünmeyen mürekkepler kullanarak farklı gizleme teknikleri geliştirmişlerdir. Bu mürekkepler genellikle meyve özü (limon gibi) ve sütten gibi doğal maddelerden oluşmaktadır. Isıtılınca ortaya çıkan bu gizli mesajlaşma tekniği günümüzde de hala kullanılmaktadır. İkinci Dünya Savaşı sırasında Almanlar tarafından mikro–nokta (microdot) olarak adlandırılan farklı bir gizleme tekniği geliştirilmiştir. Bu teknikte alfabede kullanılan noktalama işaretleri içerisine ebatları küçültülmüş fotoğrafik bir takım gizli mesajlar gömülerek teknik çizimleri de içeren geniş miktarda basılı bilgi gönderilebilmiştir.

Dünya savaşları sırasında steganografinin yaygın kullanımı ve şüphelenme atmosferi içerisindeki İngiltere ve ABD tarafından posta yolu ile her türlü satranç oyunu, örgü işleme resimleri, gazete kupürleri, çocukların çizimleri gibi gizli veri taşıması muhtemel dokümanların gönderilmesi kısıtlanmıştır. Yine aynı dönemde Sovyetler Birliği (SSCB) tarafından da tüm uluslararası postalar casusluk aktivitelerine karşı sürekli olarak taranmıştır. Bilgisayar teknolojisinin hızla gelişmesi ile birlikte bu

sınırlamaların neredeyse tümü geçerliliğini kaybetmiştir. Çünkü günümüzde herkes steganografinin üstünlüklerini kullanabilir hale gelmiştir (Çetin, 2008).

Temeli antik çağlara kadar dayanan gizli haberleşme, teknolojik ilerlemeler ile birlikte şekil ve yöntem açısından faklılıklar göstermiş olup, önemini sürekli olarak korumuştur. Gizliliğin çok önemli olduğu uygulamalarda; korunan bilgilerin, üçüncü şahısların eline geçmeden ilgili hedefe gönderilmesi amaçlanır ve bu yönde çalışmalar yapılır. Sonuç olarak veri gizleme sanatı, çağlar boyunca insanların ilgisi ve ihtiyacı ile giderek gelişmiş olup günümüzde önemli bir bilim dalı haline gelmiştir.

2.4.2. Sayısal imgelerde steganografi

Sayısal imgelerin görünümünde ciddi anlamda bozulmalara neden olmadan önemli bir veri gizlenmek istendiğinde, örtü dosyasının piksel değerleri üzerinde çalışma yapılarak gürültü ile yer değiştirilmesi sağlanır. Sayısal imge içerisine önemli bir veri gizlemek için kullanılan yöntemler genellikle örtü dosyası üzerinde en düşük öneme sahip bitleri (LSB: Least Significant Bits), maskeleme, algoritma ve dönüşüm tekniklerini kullanırlar.

Sayısal imge içerisine veri gizleme yöntemleri algoritma düzlemine göre iki kategoride sınıflandırılabilir. Bunlardan biri “bit uzayında” veri gizleme, diğeri ise “frekans uzayında” veri gizlemedir. Bit uzayında veri gizleme işlemi sırasında, gizli veri resim pikselleri içerisine doğrudan yerleştirilir. Frekans düzleminde ise, öncelikle örtü dosyası frekans düzleminde ifade edilir daha sonra gizlenecek veri taşıyıcı resmin dönüşüm katsayılarına yerleştirilir.

2.4.2.1. Bit uzayında steganografi

Bit uzayında–düzleminde veri gizlemek için ilk ve en çok kullanılan teknik “en düşük değerlikli bit – LSB” tekniğidir. LSB yönteminin popüler olmasının ve sıklıkla kullanılmasının en önemli nedeni uygulanmasının çok kolay olmasıdır. Bu yöntemde, içerisine veri gizlenmek istenen örtü dosyası pikselleri ve gizlenmek

istenen veri, ikili sayı (binary) formatında ifade edilir. Bu işlemden sonra, gizlenmek istenen verinin her bir bit değeri (1 veya 0) taşıyıcı resmin her bir pikselinin en düşük değerlikli bit değeri ile değiştirilir. Bilgi gizlemek için kullanılabilecek en iyi resim formatı 24–bit Bitmap (BMP) resimdir. Bunun başlıca sebebi bu resim formatının yüksek kaliteye sahip olması ve gizlenebilecek veri kapasitesini maksimum seviyeye çıkarmasıdır. Veri gizleme için kullanılacak olan resim formatı yüksek kaliteye sahip olduğunda, bilginin gizlenmesi ve maskelenmesi daha kolay gerçekleştirilir (Schyndel, 1994, Wolfgang, 1996).

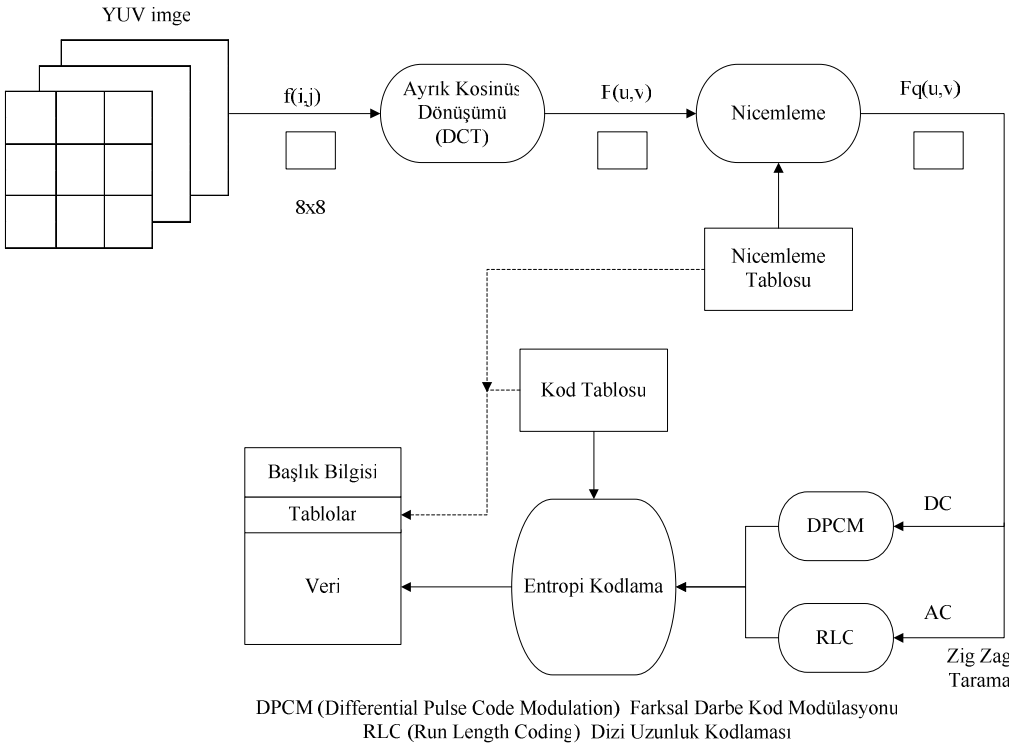
Bu teknikler tamamıyla resim formatına bağlıdır ve BMP gibi kayıpsız resim formatları üzerinde kullanılırlar. Bunun sonucunda da büyük miktarda veri gizlemek için oldukça büyük kapasiteye sahip örtü dosyası gereksinimi ortaya çıkar. Literatürde bit uzayında yapılmış olan birçok çalışma mevcut olup (Tian, 2003, Liang ve diğ., 2007, Tsai ve diğ., 2009) geliştirilen kimi yöntemlerin patentleri de alınmıştır (Barton, 1997, Honsinger ve diğ., 2001).

Sadece 24–bit imgelerle sınırlı olmayan veri gizleme uygulamaları piksel değerleri yalnızca 0 veya 1 değerini alabilen imgelere de uygulanabilmektedir (Ho ve diğ., 2009, Kim ve Queiroz, 2004).

2.4.2.2. Frekans uzayında steganografi

Bir bilgiyi resmin içerisine gizlemenin en karmaşık yolu ayrık kosinüs dönüşümü (DCT), ayrık dalgacık dönüşümü (DWT) ve ayrık fourier dönüşümü (DFT) gibi dönüşüm yöntemleri kullanmaktır. Bu yöntemler örtü dosyasının önemli bölgelerinde bulunun piksellerinin ayrık kosinüs, ayrık dalgacık veya ayrık fourier dönüşüm katsayılarında değişiklik yaparak gizlenecek bilgiyi frekans düzleminde gömerler. Gerekirse parlaklık gibi örtü dosyasının bazı özelliklerini değiştirerek algılanabilirliği engellemeye çalışırlar. Burada bahsedilen örtü dosyasının önemli bölgelerinden kasıt şudur; bir resme ayrık kosinüs dönüşümü uygulandıktan sonra matematiksel olarak resim bileşenlere ayrılır. Her bir bileşene ait sabit bir katsayı çarpanı bulunur. Bu katsayılardan bazıları matematiksel olarak sıfır değerinde, bazıları ise sıfırdan farklı değerdedir. Bunun anlamı ise sıfır değerine sahip olan

bileşenler İGS tarafından algılanamayan bölgelerdir ki bu bölgeler kayıplı sıkıştırma yöntemlerinde resim içerisinden atılarak sıkıştırma işlemi gerçekleştirilir (Şekil 2.5). Sıfırdan farklı değere sahip bileşenler, resim içerisinde İGS'de algılanabilir bölgeleri temsil etmektedirler. Bu yöntemde bilgi gizleme için bu bölgeler kullanılır. Birçok dönüşüm boyutunu kullanan veri gizleme yöntemi, örtü dosyası formatından bağımsızdır. Böylelikle kayıplı ve kayıpsız resim formatları arasında yapılacak dönüşümler sırasında gizli veri kaybolmayacaktır. Bu tekniklerde gizlenebilecek bilgi miktarının kapasitesi ile saldırılara karşı dayanıklılık kontrol edilebilir (Venkatraman ve diğ., 2004).



Şekil 2.5: JPEG kodlayıcı yapısı.

2.4.3. Sayısal seste steganografi

İnternet üzerinde yaygın şekilde kullanılmaları ve kolaylıkla paylaşılabilmeleri nedeniyle ses dosyaları da veri gizleme işlemlerinde örtü verisi olarak kullanılmaktadır. Ancak İDS, İGS'ye oranla daha hassastır (Erçelebi ve Subaşı, 2005). Bu sebeple oluşturulan bozulmaların en düşük seviyede tutulması büyük

önem taşır. Ses dosyaları için birçok veri gizleme yöntemi geliştirilmiştir. Bu çalışmalardan önemli olan bazıları şunlardır;

− Düşük bit kodlama,
− Yankı gizleme,
− Yayılı izge.

2.4.3.1. Düşük bit kodlama

Genellikle ses dosyası içerisine veri gizlemek için LSB metodunda olduğu gibi düşük değerlikli bitler kullanılır (Yalman ve Ertürk, 2008). Fakat bu yöntemin kullanılmasında karşılaşılan genel sorun, insan kulağının ses dosyalarındaki bozulmalara karşı nispeten daha hassas olmasıdır. Ayrıca bu yöntemde haberleşme kanalında oluşabilecek gürültü nedeniyle gizli verinin kaybedilmesi olasılığı yüksektir ve haberleşmenin kayıpsız şekilde yapılması önemlidir (Akbal ve diğ., 2010).

2.4.3.2. Yankı gizleme

Yankı gizleme insan kulağının ses dosyası içerisindeki kısa süreli yankıları (milisaniyeler mertebesinde) algılayamaması özelliğini kullanan yeni bir dönüşüm kodlama tekniğidir. Bu yöntemde, ses dosyası içerisine bilgi gizlemek için ilgili dosyanın içerisindeki yankılardan faydalanır. Gecikme ve bağıl genlik değerlerine göre ses dosyasının içerisine yankı sinyali eklenir. Gömü verisi ise bu yankı sinyali içerisine ‘0’ ve ‘1’ olarak kodlanır. Gecikme zamanı 0,5 ms ile 2 ms arasında, bağıl genlik ise yaklaşık 0,8 olarak seçilir ve işlemler gerçekleştirilir (Gruhl ve diğ., 1996).

2.4.3.3. Yayılı izge

Yayılı izge (spread spectrum) modülasyonu ses dosyalarında kullanılan bir başka gizleme yöntemidir. Bu yöntem frekans boyutunda ses sinyaline rasgele gürültü ekleyerek veri gizleme işlemini gerçekler (Malvar ve Florencio, 2003). İletişim kanalında meydana gelebilecek olası kayıplara ve saldırılara karşı dayanıklı olmakla

birlikte insan duyma sistemi tarafından algılanabilecek büyüklükte gürültüye neden olması sebebiyle güvenli değildir.

2.4.4. Hareketli görüntü (video) kayıtlarında steganografi

Kapasite problemi, veri gizleme tekniklerinde sürekli olarak araştırmacıları üzerinde düşündürmüş ve aşılması gereken bir zorluk olmuştur. Hareketsiz görüntülerin kapasiteleri belli bir sınırın ötesine geçemediğinden araştırmalar oldukça fazla gömü verisi kapasitesine imkân sağlayan hareketli görüntü kayıtları (video) üzerinde yoğunlaşmıştır. Video dosyalarına bilgi gizlemek için genelde resim ve ses içerisine bilgi gizleme yöntemleri birleştirilerek kullanılır. Bilindiği gibi video dosyası hareketsiz resimlerin ardı sıra oynatılmasından meydana gelmektedir. Böylelikle resim dosyaları içerisine veri gizleme için kullanılan yöntemler video dosyaları içinde kullanılabilmektedir. Genellikle video dosyaları içerisine veri gizlemek için dönüşüm–boyutu yöntemleri (Discrete Cosine Transform–DCT, Discrete Wavelet Transform–DWT gibi) kullanılır. Örneğin DCT yöntemi video dosyasını oluşturan her bir hareketsiz resmin önemsiz miktarlarda değiştirilmesi esasına göre çalışır. DCT resim içerisindeki değişmeyen noktaların değerlerini yukarıya yuvarlayarak değiştirir. Örneğin 8,779 değerine sahip bir noktanın değeri yuvarlama işleminden sonra 9 olacaktır. Video dosyasındaki ses bilgisi içerisine bilgi gizlemek için de yine ses dosyalarında kullanılan yöntemlerin kullanılması kapasiteyi arttırıcı bir yöntem olacağı gibi animasyon dosyalarında da veri gizleme işlemi yapılarak gizli haberleşme gerçekleştirilebilir (Tadiparthi ve Sueyoshi, 2008).

2.4.4.1. Ham videolarda steganografi

Video dosyasının bilgi gizleme için kullanılmasının en büyük yararlarından biri çok büyük miktarda gizli veri kapasitesi sağlamasıdır. Örneğin 30 fps (frame–per–second) ve 10 saniyelik bir video dosyası 300 hareketsiz resimden oluşmaktadır. Böylece bir resim dosyası içerisine gizlenecek gizli veri kapasitesi bu örnek video dosyası için 300 kat daha fazla olacaktır. Diğer taraftan, videoyu oluşturan her bir imgede veri gizleme yönteminden kaynaklanabilecek muhtemel bozukluklar İGS tarafından fark edilemeden görüntü akmaya devam edecektir. Video dosyasının

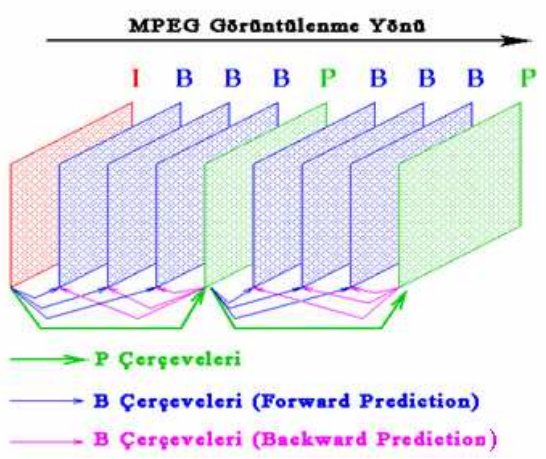
gerçek zamanlı elde edilmesi durumunda ise veri gizleme uygulamasına örtü oluşturan çerçeveler herhangi kimsede bulunmayacağından güvenlik oldukça arttırılmış olacaktır (Shahreza, 2006, Brunton ve Zhao, 2005).

Bir hareketli görüntü (video) içerisine gizli veri, her bir çerçeve ayrı ayrı kullanılarak gömülebilir. Var olan hareketli görüntü içerisine veri gizleme yöntemlerinin birçoğu imge içerisine veri gizleme yöntemleri ile tamamen benzer bir işleyişe sahiptir. İlk olarak video dosyaları üzerinde yapılan veri gizleme çalışmaları ham (raw–video) videolar üzerine odaklanmıştır. Ham videolar üzerinde yapılmış birçok veri gizleme uygulaması ve çalışması vardır. Bu çalışmalar video içerisine bilgi gizleme çalışmalarının temelini oluşturan çalışmalardır. Sonraları ise gerek ilerleyen sıkıştırma teknikleri ve gerekse büyük kapasiteye sahip videoların internet üzerinden iletimleri sırasında gerektirdikleri yüksek bant genişliği gereksinimi gibi sıkıntılar çalışmaların sıkıştırılmış (bit–stream) videolar üzerine kaymasına neden olmuştur.

2.4.4.2. Sıkıştırılmış videolarda steganografi

Günümüzde internet teknolojisinin büyük bir hızla gelişmesi ve internet kullanıcısının geçmiş yıllara nazaran hızla artması birçok uygulamanın internet tabanlı olması gerekliliğini artırmıştır. Ayrıca ağ teknolojilerindeki bu hızlı ilerleyiş müzik, resim ve video gibi birçok sayısal dosyanın insanlar arasında kolaylıkla paylaşılabilmesine olanak sağlamıştır. Yüksek boyutlardaki dosyaların paylaşımı için sistem ve bağlantı kaynaklarının yeterli olmaması durumunda kullanılmak üzere, araştırmalar sıkıştırma teknikleri üzerinde yoğunlaşmış ve birçok standart geliştirilmiştir. Görüntü için en çok bilinen sıkıştırma standardı MPEG (Moving Pictures Experts Group–Hareketli Görüntüler Uzmanları Gurubu)'dir. MPEG formatındaki bir videoya gizli veri gömerken DCT yöntemi kullanılır (Barni ve diğ. 2005, Candan, 2004). MPEG formatındaki bir video; I, P ve B çerçevelerinden meydana gelir (Şekil 2.6). I–çerçeve, bir önceki ve sonraki çerçevelerden bağımsız olarak tek bir resimmiş gibi kodlanır ve MPEG dosya içerisinde en fazla yer kaplayan çerçeve tipidir. MPEG dosyaları içerisine veri gizleyen algoritmaların büyük çoğunluğu I–çerçeveyi örtü verisi olarak kullanırlar (Moradi ve Gazor, 2005, Liu ve Chang, 2005). P–çerçeve, bir önceki çerçevedeki farklılıkları belirtir.

Görüntülenebilmesi için bir önceki ve bir sonraki çerçeveye ihtiyaç duyar. B–çerçeve ise, hem önceki hem de sonraki çerçevelere bağımlı olarak kodlanır ve I–çerçevenin %25'lik bölümünü içerir.



Şekil 2.6: Mpeg dosyalarının yapısı.

Litertürde sıkıştırılmış videolar için çeşitli yöntemler geliştirilmiştir. İGS'nin hareket eden hızlı nesnelere ait detayları algılayamamasından faydalanarak hareketli bölgelere veri gömen (Lee ve diğ., 2000), bütün çerçevelere aynı ya da farklı gömü verisinin gizlenmesini esas alan (Doerr ve Dugelay, 2004), MPEG–2 dosyalarına (Dai ve diğ., 2003) ve H264 tipindeki video dosyalarına veri gizleyen (Zlomek, 2007) yöntemler bunlardan sadece bir kaçıdır. Sıkıştırılmış video içerisine bilgi gizleyerek kolay dağıtım ve paylaşım gibi problemlere çözüm aranırken, kapasitenin düşmüş olması ise başka bir problemi ortaya çıkarmaktadır. Sıkıştırma algoritmalarının gereği olarak, sıkıştırılan dosya içerisindeki insan gözünün veya kulağının algılayamadığı bilgiler kalıcı olarak silinir. Bunun anlamı ise bilgi gizleme için kullanılacak olan örtü dosyasının boyutunun azalması ve sonuç olarak gizlenecek bilginin boyutunun azalmasıdır.

2.5. Sonuç

Haberleşme bilgilerinin anlamsız karakter ya da dizilerden oluşturulmasını esas alan yöntem şifreleme olarak adlandırılır. Şifrelenmiş bir verinin en zayıf yönü, verilerin gözlemlenmesi sonucunda haberleşmenin şifreli olduğunun anlaşılmasıdır.

Haberleşmenin şifreli ya da gizli olduğu kuşkusu yetkisiz kişiler tarafından anlaşıldığında ise gizli veriye yapılacak muhtemel saldırılar gündeme gelecektir.

Olası saldırılara maruz kalmamak için haberleşmenin de gizli olarak yapılması gerekliliği ortaya çıkar ki bu durumda haberleşme bilgilerinin maskelenmesi yoluna gidilir. Aynı zamanda bu yöntem veri gizleme olarak da bilinir. Bu yöntemde, şifrelemenin zayıflığı olarak nitelendirilen, şifreli haberleşme bilgilerinin gözlenerek fark edilmesi ve düzenlenecek saldırıların engellenmesi amaçlanır. Veri gizleme yöntemlerinde en kritik nokta, yapılan saldırılardan korunmak değil saldırıların yapılmasını önlemektir. Veri gizleme yöntemleri gizli verilerin masum görünümlü taşıyıcılar ile gönderilmesi ilkesine dayanmaktadır. Damgalama popüler medya içerisine veri gizleme/steganografi işleminin yapılması olarak tanımlanabilir ve saldırılara karşı dayanıklı olması beklenir. Steganografi ise teknik olarak, bir veriyi ya da mesajı başka bir nesnenin içerisine gizli biçimde yerleştirmeyi esas almaktadır. Öyle ki, sadece belirlenen alıcı, kendisine iletilmek istenen veriyi ya da mesajı nesneden seçebilmekte ve diğer gözlemcilerin o nesnenin içindeki mesajın varlığından haberleri olmamaktadır.

Tez çalışması kapsamında güvenli bir iletişim gerçekleştirmek için, gizli veriler HSV yöntemi kullanılarak sayısal görüntülere ve gerçek zamanlı sıralı imgelerden oluşan hareketli görüntü kayıtlarına uygulanmaktadır. Hareketli görüntülere HSV'nin uygulanması sonucunda örtülü dosyalar muhtemel ataklardan korunmakta ve oldukça büyük gömü verisi kapasitesi sağlanmaktadır.

3. SAYISAL GÖRÜNTÜ TEMELLERİ VE GÖRÜNTÜ İŞLEME

3.1. Giriş

Bilgi teknolojilerinin hızla gelişmesi ve çoklu ortam özelliklerine sahip elektronik cihazların artması ile sabit/hareketli görüntülerin (resim/video) sayısal ortamda saklanması önemli bir ihtiyaç haline gelmiştir. Sayısal görüntü; arşivleme, korunma ve yayımlanma gibi birçok alanda işlem kolaylığına sahip olduğundan, hızla analog görüntülerin yerini almıştır. Bu bölümde insan görme sistemi ve görüntülerin elektronik ortamlara aktarılmasına ilişkin detaylar verilmektedir.

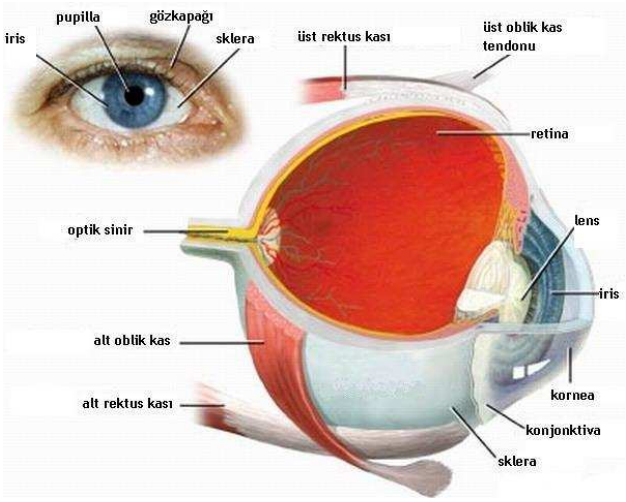
3.2. İnsan Görme Sistemi (İGS)

Görüntü işleme teknikleri insanın görsel algılama kabiliyeti doğrultusunda geliştirilmektedir. Bu nedenle İGS yapısının ve sınırlarının bilinmesi birçok noktanın anlaşılmasında faydalı olacaktır. Çünkü sayısal görüntülere veri gizleyen yöntemler İGS'nin algılamadaki hassasiyetinin nispeten daha az olmasından faydalanmaktadır.

3.2.1. Gözün yapısı

İnsan gözünün yapısı temel olarak; kornea, iris, göz bebeği (pupil), göz merceği (lens), ağ tabaka (retina), fovea, koroid (choroid), göz akı (sclera) ve optik sinirlerden oluşmaktadır (Pratt, 2007). Yarı şeffaf bir yapıya sahip olan kornea gözün ön bölümünü kaplamaktadır. Gözün en dışındaki koroidi kaplayan ve lifli bir tabakadan oluşan göz akı (sclera) aynı zamanda kılcal kan damarlarını içeren bir katmandır. Koroidin iç kısmı ise retina yani ağ tabakadır. Ağ tabaka; çubuk (rod) ve koni (cone) adı verilen iki tip algılayıcıdan oluşmaktadır. Ağ tabakanın sinirlerle bağlantısı gözün arka tarafındaki optik sinir yığınları ile sağlanır. Göz merceği nesnelerin uzaklığına ya da yakınlığına göre şekil değiştirerek odaklanmayı sağlar. Merceğin merkezi ile ağ tabaka arasındaki mesafe yaklaşık olarak 17 mm'dir. Göze

rengini veren iris, nesneden gelen ışığın şiddetine göre göz bebeğinin genişlemesini ya da küçülmesini sağlayan bir kas dokudan oluşmaktadır (Şekil 3.1). Bu yönüyle iris bir bakıma diyafram vazifesi görmektedir.



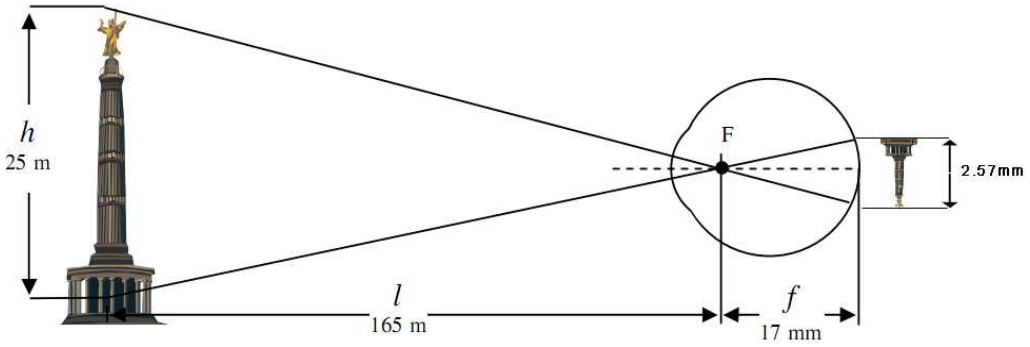
Şekil 3.1: İnsan gözü ve bölümleri.

Gözün odaklandığı bir nesneden gelen ışık, korneadan geçerek ağ tabaka üzerine düşer. Bir nesnenin algılanmasında, ağ tabaka üzerinde bulunan çubuksu ve konisel algılayıcıların çok büyük önemi vardır. Çubuk algılayıcıları ışığa daha hassas olup daha narin ve uzundurlar ve sayıları yaklaşık 75–150 milyon civarındadır. Daha kısa ve kalın yapıda olan koni algılayıcıları ise ışığın renk bileşenine hassastırlar ve sayıları yaklaşık 6–7 milyondur. Yakın geçmişte, retinadaki konik algılayıcıların 3 temel tipinin olduğu deneysel olarak belirlenmiştir. Bu farklı türdeki algılayıcılar, optik spektrumun kırmızı, yeşil ve mavi gibi farklı dalga boylarında farklı tepe emilimine sahiptirler. Bahse konu olun bu üç tip algılayıcı, renkli görünün üç renkli teorisinin fiziksel temelini oluşturmaktadır. Klasik insan renkli görü sistemi modeli 1802'de Thomas Young tarafından önerilmiştir. Bu sistemdeki üç renkli model insan gözünün farklı dalga boylarına (bantlarına) duyarlı üç farklı algılayıcıya sahip olduğunu varsaymaktadır. Koni algılayıcılarının % 65'i kırmızı, % 33'ü yeşil ve geriye kalan % 2'si ise mavi rengin algılanmasında işlev görürler. Bu durum mavi rengin algılanma hassasiyetinin kırmızı ve yeşil renklere göre daha düşük olduğu anlamına gelmektedir.

Koni algılayıcılarının en yoğun olduğu ve renk duyarlılığı en yüksek olan nokta foveadır. Görüntünün algılanmasında önemli bir yeri olan fovea yaklaşık 1,5 mm çapında yuvarlak bir yapıya sahiptir. Benzer şekilde görüntü işleme tekniklerinde bir görüntünün algılanması için 1,5mm × 1,5mm boyutlarında kare veya dikdörtgen dizi yapıları kullanılmaktadır (Gonzalez ve Woods, 2002). Fovea'nın boyutlarına göre ağ tabaka'nın merkezindeki koni yoğunluğu mm^2 başına yaklaşık olarak 150.000 elemandır. Fovea merkezinde bulunan en hassas bölgedeki koni sayısı yaklaşık olarak 1,5×1,5×150.000 =337.500 elemandır. Sayısal kameralarda kullanılan görüntü yongasının (CCD: Charge–Coupled Device) çözünürlük hassasiyeti için bu hesaplamalar önemli bir yer tutmaktadır. Örneğin, iyi görüntü kalitesi için görüntü yongasının algılayıcı dizisi 5mm×5mm'den büyük olmamalı ve en az yukarıda verilen sayıda eleman içermelidir (Gonzalez ve Woods, 2002, Çetin, 2008). Sayısal imgelere veri gizleme işleminin sağlıklı şekilde yapılabilmesi için öncelikle görüntü kalitesinin iyi olması istenir. Orijinal görüntü kalitesini elde etmek için yukarıda belirtilen asgari şartlar sağlandıktan sonra elde edilen sayısal görüntüler kullanılmalıdır.

3.2.2. Görme olayının gerçekleşmesi

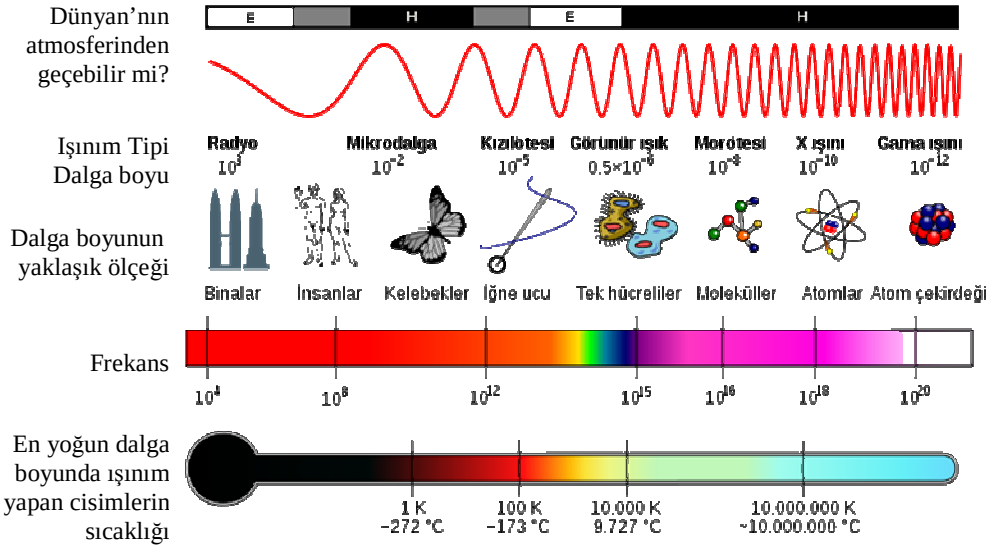
Görme olayının gerçekleşmesi için gerekli olan en önemli şart, ortamda bir ışık kaynağının olmasıdır. Nesnelerden yansıyarak korneadan göze giren ışık görme eyleminin gerçekleşmesi için önemli bir aşamanın geçilmesini sağlar (Şekil 3.2). Korneanın kavisli bir yapıya sahip olması ile ışık korneadan kırılarak geçer. Gözün bir nesneye ya da noktaya odaklanmasını ise göz merceği sağlar. Göz merceğinin hareketi göz kapağındaki liflerin elektriksel sinyalleri ile kontrol edilir. Göz merceği uzaktaki nesnelere odaklandığında kırma olayını en düşük seviyede gerçekleştirir. Yakın mesafedeki nesnelere odaklandığında ise tam tersi yani en yüksek seviyede kırma yapar.



Şekil 3.2: İnsan gözünde görüntü oluşumu.

3.3. Işık ve Elektromanyetik Tayf

Işık, gözün görme işlemini gerçekleştirmesinde çok önemli bir rol oynayan elektromanyetik bir radyasyon türüdür. 1666 yılında Newton, beyaz güneş ışığını cam bir prizmadan geçirerek ışık tayfını keşfetmiştir. Newton'un elde ettiği mordan kırmızıya kadar farklı renklerden meydana gelen bu ışık tayfı gökkuşağı renkleri olarak da bilinmektedir. Şekil 3.3'te verilen elektromanyetik tayfa bakıldığında, görülebilir ışığın dalga boyu, tayfın çok küçük bir bölümü olan 350 nm−780 nm değerleri arasındadır (Bothun, 2010).



Şekil 3.3: Elektromanyetik tayf.

Elektromanyetik tayf; dalga boyu, frekans veya enerji ile ifade edilebilir. Dalga boyu (λ) ve frekans (f) arasında aşağıda görüldüğü gibi bir bağlantı vardır;

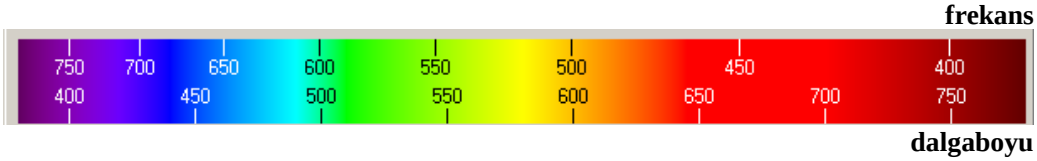
$$\lambda = \frac{c}{f} \tag{3.1}$$

Yukarıda verilen *c*, ışık hızını (2,998 $\times 10^8$ m/s) göstermektedir. Enerji (E) ile frekans arasındaki ilişki ise aşağıdaki gibidir (h=Planck sabiti (6,63$\times 10^{-34}$ Joule.sn)).

$$E = h \times f \tag{3.2}$$

3.3.1. Görülebilir tayf

Görülebilir tayf, elektromanyetik tayfın bir parçasıdır ve görülebilir ışık veya sadece ışık olarak adlandırılır. Bu alanın görülebilir olarak adlandırılmasının sebebi, elektromanyetik tayf üzerindeki diğer enerji biçimlerinden farklı olarak insan gözü tarafından algılanabilmesidir. Görülebilir ışığın sahip olduğu frekans aralığı dışında frekans yayan dalgalar ise İGS tarafından algılanamamaktadır (morötesi, kızılötesi vb.) (Şekil 3.4).



Şekil 3.4: Görülebilir ışıklar ve dalga boyları.

Elektromanyetik tayfta görülebilir alanın dalgaboyu değerleri Şekil 3.4'te de görüldüğü gibi 350 nm (mor) ile 780 nm (kırmızı) arasındadır. Her bir renk farklı bir dalga boyuna sahiptir. Kırmızı renk en uzun dalga boyuna sahip iken mor renk ise en kısa dalga boyuna sahiptir. Bu aralıktaki renkler ise sırasıyla; mor, mavi, yeşil, sarı, turuncu ve kırmızıdır.

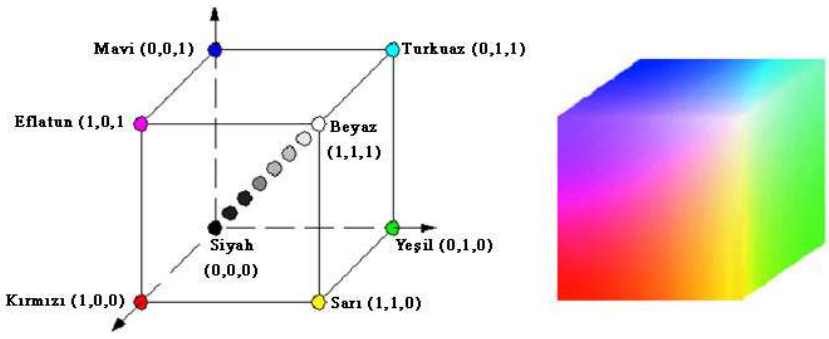
3.3.2. Renk teorisi ve renk modelleri

Üç renkli görü (trichromatic) teorisinin temeli, üç temel rengin doğru oranlarda birleştirilmesi ile istenilen herhangi bir rengin elde edilmesidir. Örneğin renkli

televizyon sisteminde de kullanılan toplamsal renk yaklaşımı ile üç temel renk olan kırmızı, yeşil ve mavi ortak bir noktaya yansıtılarak istenilen renkte bir ışık elde edilebilir. Renkli fotoğraf ve renkli yazıcılar sistemlerinde de kullanılan farksal renk sisteminde, beyaz ışık sırasıyla turkuaz veya camgöbeği (cyan), eflatun (magenta) ve sarı (yellow) filtrelerden geçirilerek istenilen renkli bir ışık elde edilmektedir.

3.3.2.1. RGB renk modeli

RGB renk modeli, fosfor yapıların ışık yayması prensibine dayanarak oluşturulmuş, toplamsal (additive) bir renk modelidir. Bu renk modelinde ana renkler olarak kırmızı (red), yeşil (green) ve mavi (blue) kullanılır. Modelin ismi de bu renklerden gelmektedir. Diğer renkler belirtilen üç ana rengin belli oranlardaki karışımından elde edildiği için bu renk modeli toplamsal renk modeli olarak da ifade edilir. Beyaz renk kırmızı, yeşil ve mavi renklerin hepsini içermekte, siyah ise hiçbirini içermemektedir (Şekil 3.5). Bu model genellikle televizyon, bilgisayar ekranı gibi aktif göstergelerde kullanılır.



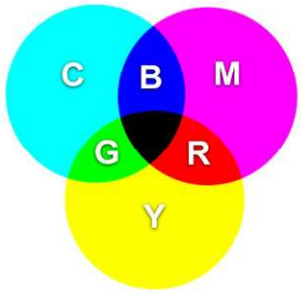
Şekil 3.5: RGB renk modeli.

İnternet veya sayısal ortamlarda yapılan çalışmalarda RGB renk modelinin kullanılması bir avantajdır. Baskı ortamında yapılan çalışmalar için ise CMYK renk modeli geliştirilmiş ve matbaacılıkta bir standart halini almıştır.

3.3.2.2. CMYK renk modeli

RGB çok yaygın olarak kullanılmasına rağmen, tertibata çok bağımlıdır. Tertibatın değişmesiyle renk de değişir. Bu renk modelinin tarayıcı, monitör, yazıcı gibi

aygıtlarla beraber kullanımı uygun değildir. Baskıda kullanılan 4 ana renk vardır (turkuaz (cyan), eflatun (magenta), sarı (yellow) ve siyah (black)). Belli açılara ve değerlere sahip bu renkler, üst üste basılarak tüm ara renkler ortaya çıkarılır (Şekil 3.6). Örneğin kırmızı (R) renk M ve Y'nin tanımlanmış olan teknikle üst üste basılması ile oluşturulur.



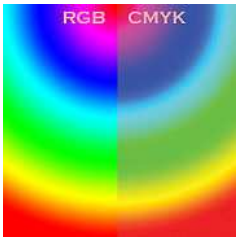
Şekil 3.6: CMYK renk modeli.

Bu renk modelinde RGB renk modelinin tersine diğer renkleri elde etmek için bir nevi çıkarma işlemi uygulanır. Çıkarma işleminin kullanılması sebebiyle eksiltici (subtractive) renk modeli olarak da ifade edilir. Diğer renklerin elde edilmesinde, hangi renk için hangi ana renklerin emilmesi veya yansıtılması gerektiği Tablo 3.1'de verilmektedir. Bu işlem için renklere yansıtıcı olmayan bazı pigmentler eklenerek o rengin görülmemesi sağlanır.

Tablo 3.1: CMYK renk modelinde diğer renklerin elde edilmesi.

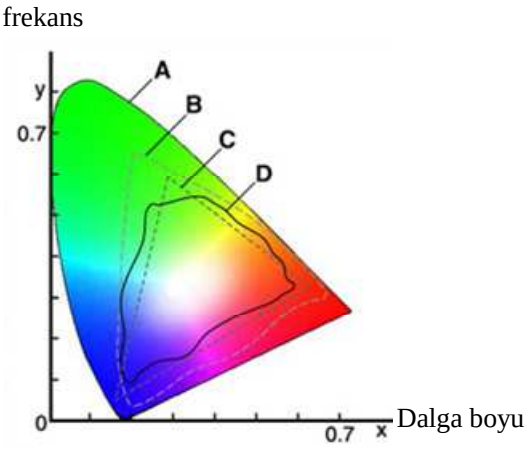
Ana Renk	**Emilme**	**Yansıtma**
Turkuaz (Cyan)	Kırmızı	Mavi ve Yeşil
Eflatun (Magenta)	Yeşil	Mavi ve Kırmızı
Sarı (Yellow)	Mavi	Kırmızı ve Yeşil
Siyah (Black)	Hepsi	Hiçbiri

Görünür ışık içinde birkaç milyon renk barındırır, ancak bu renklerin her biri bilgisayar veya basım mürekkebi tarafından üretilemez. RGB renk modelini kullanan bilgisayarlar ve tarayıcılar ile renkli yazıcılar ve CMYK renk modelini kullanan diğer baskı aletlerinin farklı bir renk serisi vardır. En düşük üretim kapasitesi CMYK renk modelinde görülür. Bir bilgisayar ekranında mükemmel görünen RGB renkleri, CMYK renk modeline çevrildiklerinde çok daha mat (solgun) görünürler (Şekil 3.7).



Şekil 3.7: RGB ve CMYK renk modellerinin karşılaştırılması.

Bu durumun nedeni ekrandaki görüntünün CMYK renk modelinde üretilemeyecek renkler kapsamasıdır (Şekil 3.8).



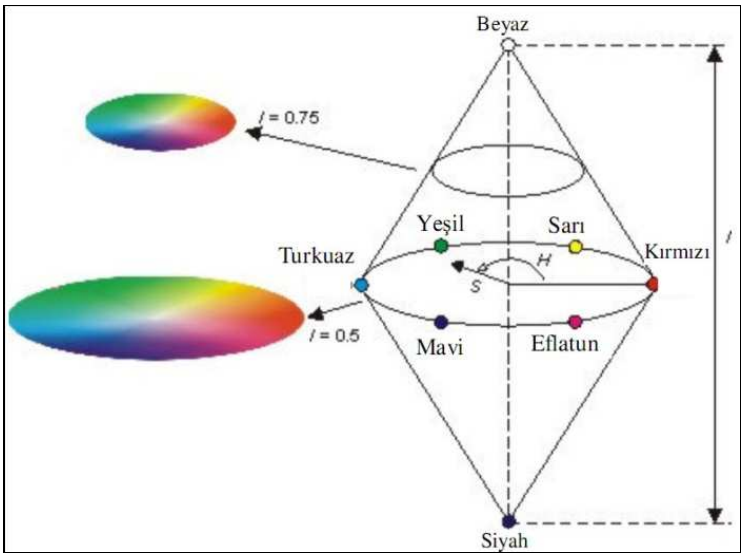
A: İnsan gözünün renk alanı
B: Renkli filmin renk alanı
C: Bilgisayar ekranının renk alanı
D: Baskı renk alanı

Şekil 3.8: Renk alanlarının karşılaştırılması.

3.3.2.3. HSI renk modeli

HSI (Hue − Saturation − Intensity = Renk − Doygunluk − Yoğunluk) renk modelinde ise yoğunluk (parlaklık/keskinlik), renk bilgisinden ayrıştırılmıştır. Renk bilgisi renk tonu (hue) kanalı ve doygunluk (saturation) kanalı ile oluşturulur. HSI renk modeli renkler üzerindeki işlemlerde daha çok sezgisel olması ve yaklaşık olarak insan görme sisteminin algı kabiliyetine yakın olması amacıyla geliştirilmiştir. Böylece interaktif uygulamalar sırasında, kullanıcıların beklentilerine cevap verebilecek şekilde renkli resimler üzerinde işlem yapılması uygun hale gelmektedir (Çetin, 2008).

Şekil 3.9'da görülen HSI renk modelinde, ton (H) bileşeni, 0–360 derece arasındaki açılarla rengi belirtir. 0 derece kırmızı, 60 derece sarı, 120 derece yeşil, 240 derece mavi ve 300 derece eflatun rengi göstermektedir. Doygunluk (S) bileşeni beyaz renk ile birleştirilecek renk miktarını gösterir ve [0…1] arasında değer alır. Şiddet (I) bileşeni ise [0…1] arasında değer alır. 0 siyah, 1 ise beyaz anlamına gelmektedir.



Şekil 3.9: HSI renk modeli.

3.3.2.4. YUV renk modeli

YUV renk modeli PAL (Phase Alternate Line), NTSC (National Television Standards Committee), SECAM (Système Electronique Couleur Avec Mémoire) kompozit renkli analog video standartlarında kullanılır. Y bileşeni ışıklılık (luma, luminance), U ve V bileşenleri ise renklilik (chrominance) bileşenleridir. YUV değerleri RGB modeli kullanılarak türetilir. Y, ortalama parlaklığı veren ve R, G, B bileşenlerinin ağırlıklı ortalaması ile elde edilen ışıklılık bileşeni; U, mavi bileşeninden Y'nin; V, kırmızı bileşeninden Y'nin çıkartılması ile elde edilen fark bileşenleridir. Sayısal imgelerde bu model YCbCr renk modeli olarak isimlendirilir.

MPEG video sıkıştırma yöntemi insan gözünün rengin parlaklığına olan hassasiyetinin rengin kendisinden daha yüksek olması özelliğini kullanır. Bu nedenle RGB–YCbCr dönüşümü gerçekleştirilir.

3.3.3. Renk modelleri arasındaki matematiksel dönüşümler

Uygulamalardaki kullanım alanlarının farklı olması nedeni ile teorik olarak da renk modelleri arasında dönüşüm yapma ihtiyacı doğmuştur. Aşağıda en çok kullanılan renk modelleri arasındaki ilişkiyi ifade eden matematiksel denklemler verilmiştir. Denklem (3.3) RGB ve CMYK renk modelleri arasındaki dönüşümün denklemini, denklem (3.4a–d) ise RGB'den HSI renk modeline dönüşümü sağlayan denklemleri göstermektedir.

$$\begin{bmatrix} C \\ M \\ Y \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{3.3}$$

$$\theta = \cos^{-1}\left\{ \frac{\frac{1}{2}\left[(R-G)+(R-B)\right]}{\sqrt{\left[(R-G)^2+(R-B)(G-B)\right]}} \right., \tag{3.4a}$$

$$H = \begin{cases} \theta & B \le G \\ 360-\theta & B > G \end{cases}, \tag{3.4b}$$

$$S = 1 - \frac{3}{(R+G+B)}[\min(R,G,B)], \tag{3.4c}$$

$$I = \frac{1}{3}(R+G+B) \tag{3.4d}$$

Denklem (3.5a–c) ise HSI renk modelinden RGB renk modeline dönüşümü sağlayan denklemleri göstermektedir.

$$(0^\circ \le H < 120^\circ) \rightarrow \quad R = I\left[1 + \frac{S\cos H}{\cos(60^\circ - H)}\right], \quad B = I(1-S), \quad G = 3I - (R+B) \tag{3.5a}$$

$$(120^\circ \le H < 240^\circ) \rightarrow \qquad H = H - 120^\circ$$

$$R = I(1-S), \quad G = I\left[1 + \frac{S\cos H}{\cos(60^\circ - H)}\right], \quad B = 3I - (R+G) \tag{3.5b}$$

$$(240^\circ \le H \le 360^\circ) \rightarrow \quad H = H - 240^\circ$$

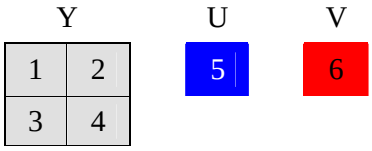
$$G = I(1-S), \quad B = I\left[1 + \frac{S\cos H}{\cos(60^\circ - H)}\right], \quad R = 3I - (G+B) \tag{3.5c}$$

Denklem (3.6a) RGB–YUV ve (3.6b) YUV–RGB renk dönüşümlerini sağlayan eşitlikleri göstermektedir.

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0{,}299 & 0{,}587 & 0{,}114 \\ -0{,}14713 & -0{,}28886 & 0{,}436 \\ 0{,}615 & -0{,}51499 & -0{,}10001 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{3.6a}$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1{,}13983 \\ 1 & -0{,}39465 & -0{,}58060 \\ 1 & 2{,}03211 & 0 \end{bmatrix} \begin{bmatrix} Y \\ U \\ V \end{bmatrix} \tag{3.6b}$$

Yukarıda verilen denklem (3.6a–b) RGB–YUV–RGB dönüşümü ICT (Irreversible Color Transform) olarak adlandırılır ve kayıplı sıkıştırma işlemlerinde (örneğin MPEG kodlama) kullanılır. Dönüşümden sonra UV değerleri için 4'e 1 oranında kayıplı sıkıştırma sağlanmış olur. Böylece Y değeri 4 birim ile ifade edilirken U ve V değerleri 1'er birim ile ifade edilir (Taşkın ve Suçsuz, 2006). Bu sayede 6 birimlik kazanç sağlanmış olur (Şekil 3.10).



Şekil 3.10: YUV kayıplı sıkıştırması.

Eğer geri dönülebilir (RCT: Reversible Color Transform) bir dönüşüm istenirse denklem (3.7a–b)'nin kullanımı daha uygun olacaktır.

$$Y = \left[\frac{R + 2\times G + B}{4}\right], \; U = R - G \; , \; V = B - G \tag{3.7a}$$

$$G = Y - \left(\frac{U+V}{4} \right),\ R = U + G,\ B = V + G \tag{3.7b}$$

Yukarıda belirtilen dönüşümler ile birlikte RGB renk modelinden gri tonlu imgelere geçişi sağlayan denklemlerde mevcuttur. Renk özü ve doygunluk bilgisi önemsenmez ise;

$$Y = \frac{R+G+B}{3}, \tag{3.8a}$$

denklemi, NTSC standardına göre dönüşüm yapılacaksa;

$$Y = 0{,}299R + 0{,}587G + 0{,}114B \tag{3.8b}$$

denklemi kullanılır (Şekil 3.11).

(a) RGB imge (b) Aritmetik ortalama ile elde edilen gri tonlu imge (c) NTSC standardına göre elde edilen gri tonlu imge

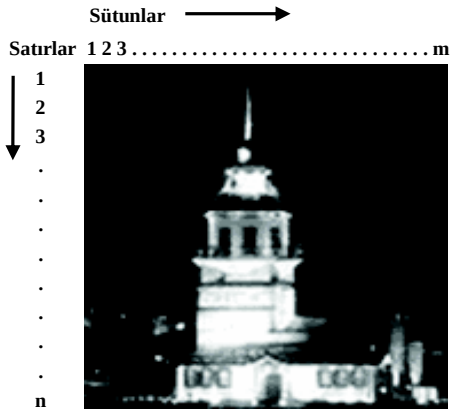
Şekil 3.11: RGB imge ve gri tonlu eşlenikleri.

3.4. Sayısal İmge ve Temel Kavramlar

Sayısal cihazların ve özellikle bilgisayarların yaygınlaşması, aynı zamanda sayısal haberleşmenin analog haberleşmeye oranla daha kolay uygulanabilir olması, tüm bilgi türlerinde olduğu gibi görüntülerin de sayısal ortama aktarılma gereksinimini ortaya çıkarmıştır. Sayısal görüntüler, özellikle internet üzerinden haberleşme de yoğun bir şekilde kullanılmaya başlanmasıyla popüler hale gelmiştir.

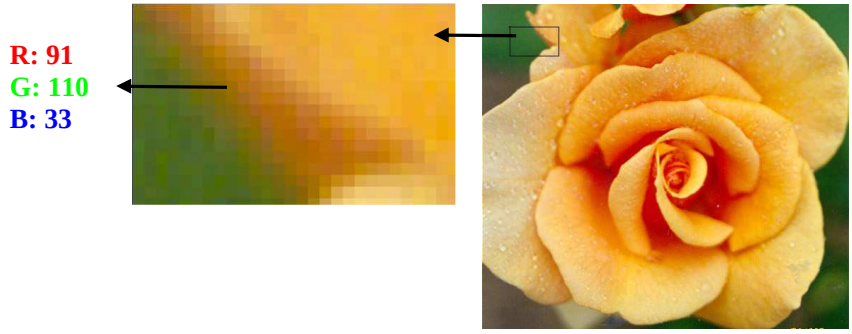
3.4.1. Piksel kavramı

Sayısal görüntü (imge, resim), n satır ve m sütunluk bir dizi ile temsil edilir (Şekil 3.12). Bir imge dizisinin elemanlarına ise piksel (picture element) denir. En basit durumda pikseller 0 veya 1 değerini alır ve bu piksellerden oluşan resimlere ikili (binary) imge adı verilir. 1 ve 0 değerleri sırasıyla aydınlık ve karanlık bölgeleri veya nesne ve zemini (nesnenin önünde veya üzerinde bulunduğu çevre zemini) temsil ederler. Sayısal görüntü dosyaları renkli olarak genellikle 24 bit (R, G, B değerlerinin her biri için 8'er bit olmak üzere), gri seviye görüntüler ise 1, 2, 4, 6 ya da 8 bit olabilirler (Yalman ve Erturk, 2009d). Bilgisayar ekranları gibi bazı sistemlerde 32–bit renk derinliği kullanılmaktadır. Buradaki fazladan kullanılan 8–bit ile opaklık yani ışık geçirmezlik değeri belirtilir.



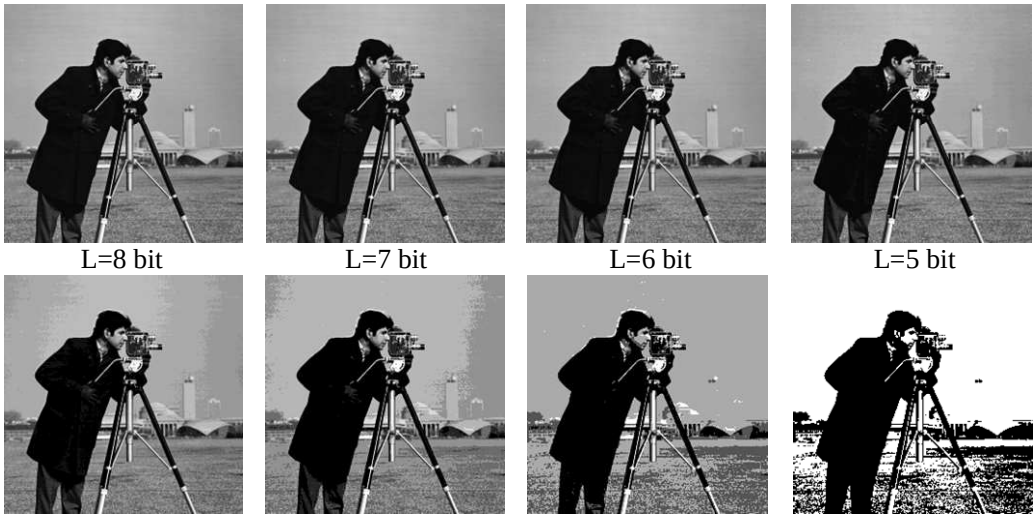
Şekil 3.12: Sayısal imgenin yapısı.

Şekil 3.13'de örnek bir sayısal imge görülmekte ve seçilen belirli bir bölgeye ait piksel haritası yakınlaştırılarak sunulmaktadır. Verilen örnek pikselden de anlaşılacağı üzere her bir pikselin rengi R, G ve B renk ağırlıklarının belli oranlarda birleşmesi sonucu oluşmaktadır. Pikseller görüntü alanını meydana getiren en küçük noktacıklardır ve ekrana bakıldığında odaklanılan görüntü alanı bütün bir resim olarak görülecektir.



Şekil 3.13: 24–bit bir imgenin piksel haritasından bir görünüm.

RGB kodlama tekniğinde her rengin bit derinliği (L) için 1 bayt (8–bit) kullanılması standart haline gelmiştir ve bir pikseli ifade etmek için 3 bayt hafıza alanına ihtiyaç vardır. Böylece her bir piksel 24–bit renk değerine sahip olur ve renk bileşeni 0–255 arasında değişen 256 farklı parlaklık değeri ile nitelendirilir. Eğer renkleri belirtmek için 4–bit kullanılırsa; her renk için parlaklık 16 (2^4) farklı şekilde ifade edilecektir ki, bu durum renkleri ayrıntılı şekilde sunmaktan uzaktır. Bit derinliği düşük olan sayısal imgeler incelendiğinde bulanık, nesne kenarları net algılanamayan (bloklama etkisinin olduğu) bir resim olarak görülür. Bununla birlikte her bir rengi belirtmek için ne kadar az bit kullanılırsa ilgili sayısal imgenin depolama biriminde kapladığı alan o oranda düşecek ve ana bellekte de o kadar az yer kaplayacaktır. Şekil 3.14'te gri tonlu bir imgenin bit derinliğinin değişmesi ile birlikte görünümünde oluşan değişim görülmektedir.



Şekil 3.14: Bit derinliği ile imge görünümü arasındaki ilişki.

3.4.2. Çözünürlük kavramı

Çözünürlük, sayısal bir imgenin yatay ve dikey olarak kaç piksel ile gösterildiğini ifade eder. Örneğin bir resim için 320×240 çözünürlüğe sahip ise; bu resim alanının yatay olarak 320 piksel, dikey olarak 240 piksel kullanılarak oluşturulduğu (320×240= 76800 piksel içerdiği) söylenebilir. Bu noktadan hareketle eşit fiziksel boylardaki sayısal imgeler için çözünürlüğü yüksek olanın gerçek görüntüye daha yakın olduğu söylenebilir.

Bir sayısal resmin bayt türünden hafızada kapladığı alan; resmin yükseklik bilgisi, genişlik bilgisi ve renk derinliği bilgileri verildiği takdirde denklem (3.5) yardımıyla hesaplanabilir;

Dosya Boyutu = (yükseklik × genişlik × renk derinliği) / 8 (3.5)

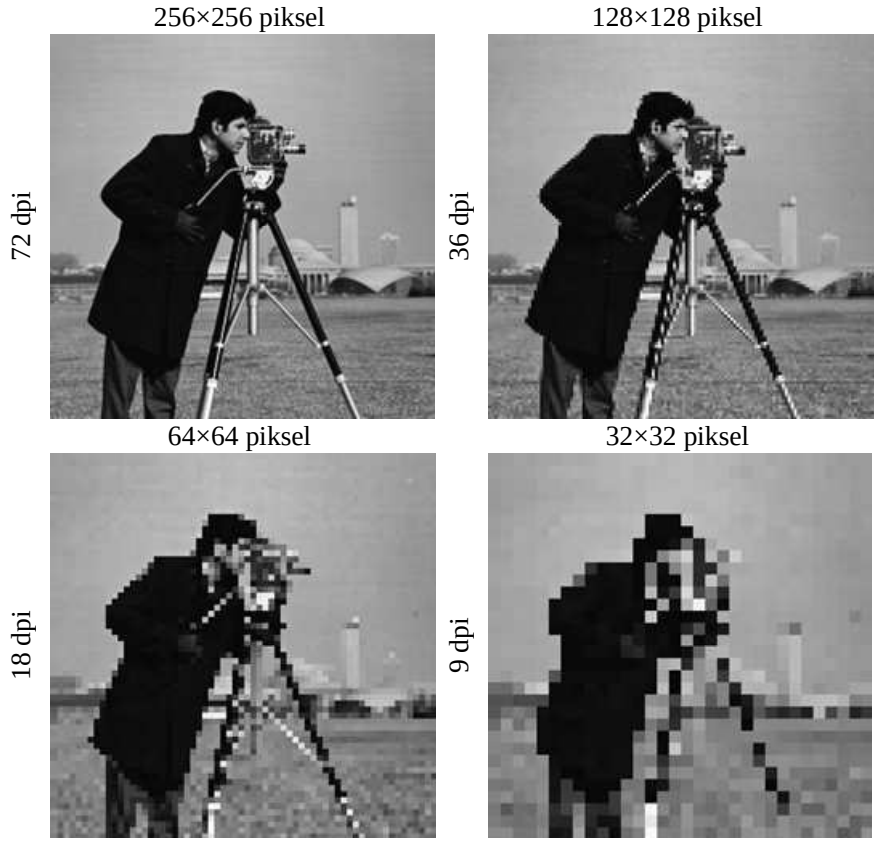
Tablo 3.2'de bazı örnek hesaplamalar verilmektedir.

Tablo 3.2: İmge dosya boyutlarının hesaplanma tablosu.

İmgenin Piksel Boyutları	Renk Derinliği	Resim Dosyası Boyutu (bayt)
256×256	8	65.536
256×256	24	196.608
320×240	16	153.600
800×600	24	1.440.000
1024×768	24	2.359.296

Bir sayısal resimde örnekleme yapılan uzamsal frekans değeri (örnekleme frekansı) çözünürlüğü göstermek için kullanılan nesnel bir ölçüttür. Genellikle örnekleme frekansını artırmak çözünürlüğü de artırır. Örnekleme, her bir inç başına düşen nokta (DPI: Dot Per Inch) sayısı veya her bir inç başına düşen piksel (PPI: Pixel Per Inch) sayısı ile ifade edilir. DPI sayısal görüntülerde çözünürlük bilgisini göstermek için kullanılan bir ölçektir. 1 inç (2,54 cm) uzunluğundaki bölgenin kaç noktadan meydana geldiğini gösterir. Örneğin, 300×300 dpi çözünürlüğündeki bir görüntünün eni ve boyu her inç başına 300 noktadan oluşur.

Şekil 3.15’te fiziksel boyutları aynı, ancak çözünürlükleri farklı olan imgelerin görünümleri verilmektedir. Şekilde görüldüğü gibi 1 inç başına düşen piksel sayısı azaldıkça görüntü kalitesi düşmekte, imgedeki detaylar anlaşılamaz hale gelmektedir.



Şekil 3.15: Çözünürlük değeri ile imge boyutu arasındaki ilişki.

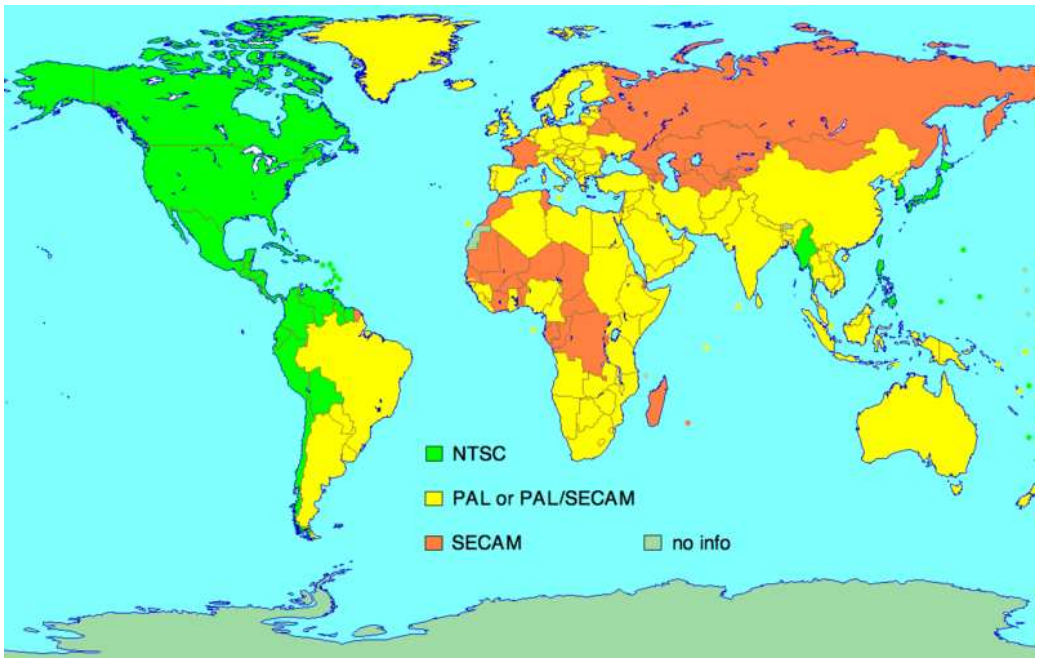
3.4.3. Görüntü sıkıştırma

Görüntü sıkıştırma özellikle depolama alanından avantaj sağlamak, dosya transferi yapmak ve görüntü işlemede kullanmak için uygulanan bir işlemdir. Bütün sıkıştırma teknikleri matematiksel ifadelerle oluşturulmuş algoritmaları kullanırlar. Kullanılan algoritmaya göre sıkıştırma işlemi kayıplı veya kayıpsız olarak adlandırılabilir. Kayıpsız sıkıştırma tekniklerinde sıkıştırma işlemi sırasında resimden herhangi bir bilgi atılmaz. Örnek olarak Uluslararası Haberleşme Birliği (International Telecommunication Union)’nin ITU–T.6 tekniği, dosya uzantısı olarak da “.bmp” uzantılı resimler gösterilebilir. Kayıplı sıkıştırma da ise, sıkıştırma işlemi sırasında resimden insan gözü tarafından algılanamayacağına karar verilen bazı bilgiler atılır.

Bu sıkıştırma formatının ismi standardı geliştiren gurubun ismi olan Birleşik Fotoğraf Uzmanları Grubu (Joint Photographic Experts Group–JPEG) ismiyle anılır.

Avrupa, Avustralya, Ortadoğu ve Afrika'nın bazı kısımlarında kullanılan, renkli televizyon yayın sistemi PAL içerisindeki teorik olarak 625 yatay satırın 576'sı görülebilirdir (Şekil 3.16). Bu durumda;

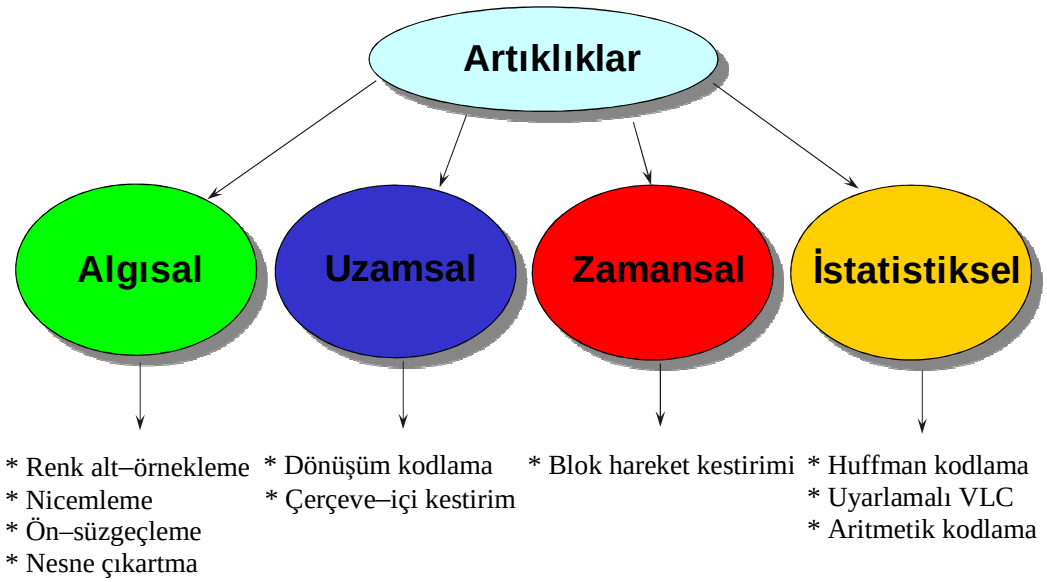
- En boy oranı: 4/3 alındığında, sütun sayısı 768 olacaktır.
- Bu durumda bir çerçeve için: 576 × 768 = 442.368 piksel gerekir.
- Saniyede 25 çerçeve için: 442.368 × 25=11.059.200 piksel/s,
- Her pikselin 8–bit ile ifade edilmesi durumunda: 88.473.600 bps,
- 3 Renkli gösterim için (RGB) : 265.420.800 bps, hıza ihtiyaç duyulur.



Şekil 3.16: NTSC, PAL ve SECAM standartlarının dünyadaki kullanım alanları.

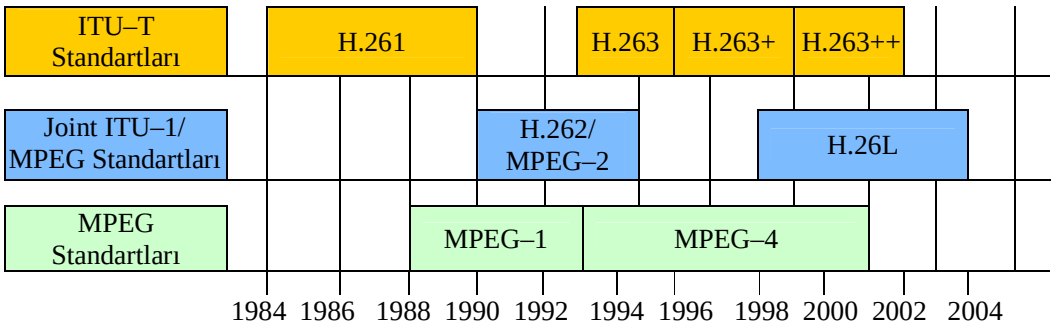
Yukarıda belirtilen hesaplamalardan hareketle tek bir televizyon kanalının iletimi için 253 Mbps gereklidir. 64–QAM modülasyonu kullanılırsa bir kanalın iletimi için gerekli bant genişliği 40 MHz'dir. Var olan analog sistemler ise bir kanalın iletimi için 5,5 MHz civarındaki bant genişliğine gereksinim duymaktadır. Bu sebeplerle sayısal görüntülerin daha kullanışlı ve paylaşımının kolay olması açısından

boyutlarının düşürülmesine ihtiyaç duyulur. Bunun için özellikle sıralı imgelerde (video) artıklıkların çıkarılması yöntemi kullanılır (Şekil 3.17).



Şekil 3.17: Sıralı imgelerde artıklıklar.

Sayısal videolardaki sıkıştırma Hareketli Resimler Uzmanlar Gurubu (Moving Pictures Experts Group–MPEG) tarafından geliştirilen standartlara göre yapılmaktadır. Resim ve video sıkıştırma için belirlenmiş video kodlama standartları Şekil 3.18'de görülmektedir.



Şekil 3.18: Video kodlama standartlarının kronolojik sıralaması.

H.261 video sıkıştırma standardı ISDN (Integrated Services Digital Network: Bütünleştirilmiş Sayısal Ağ Hizmetleri) hatlarda video konferans uygulamalarında kullanılmaktadır. ISDN hatların desteklediği bit hızı p×64 Kbps'dir. Burada p sabiti

video konferans sırasında kullanılan formata bağlı olarak değişmektedir. Genellikle video konferans uygulamalarında CIF (Common Interchange Format) formatı (352×288 çözünürlük değerinde) kullanılmaktadır.

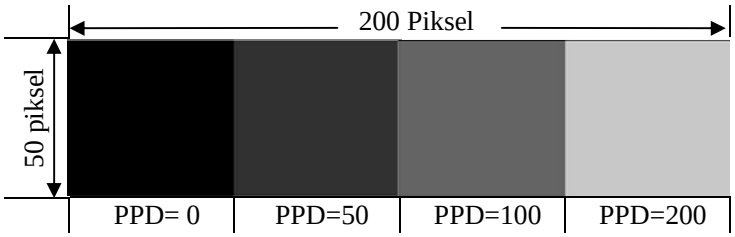
MPEG sıkıştırmada temel fikir video çerçevelerindeki uzamsal fazlalıkları ve çerçeveler arasındaki zamansal fazlalıkları silmektir. Örneğin bir sıkıştırma algoritmasında uzamsal fazlalıkları silmek için ayrık kosinüs dönüşümü (Discrete Cosine Transform–DCT) kullanılır. MPEG sıkıştırma algoritmasında görüntü renk formatı YUV renk uzayındadır. Eğer RGB renk uzayına sahip bir görüntü varsa MPEG uygulanırken renk uzayı önce YUV formatına dönüştürülür. YUV formatında da görüntüler 24–bit olarak ifade edilir. 8–bit parlaklık (Y) bilgisi için, geri kalanı ise renklilik (U ve V) için kullanılır. MPEG–1 sıkıştırma formatı CD–ROM üzerinde depolanan videolar için geliştirilmiştir. MPEG–2 ise yüksek kaliteli televizyon (HDTV–High Definition TV) uygulamalarında kullanılmaktadır. MPEG–4 standardı ise internet üzerinden gerçek zamanlı video görüşmesi yapılabilmesi için geliştirilmiştir (Tekalp, 1995).

3.5. Sayısal İmge Histogramı

Histogram, bir işlem neticesinde elde edilen ölçüm sonuçlarının dağılımını gösteren grafiktir. Analog bir işaret için histogram ilgili işaretin hangi frekans değerinde kaçar adet bileşene sahip olduğu bilgilerini verir. Bu sayede işaret bileşenlerinin hangi frekanslarda yoğunlaştığı bilgisine ulaşılır. Sayısal imge histogramı ise sayısal bir resmin renk tonlarının dağılımını gösterir (Çetin, 2008, Yalman ve Ertürk, 2009a).

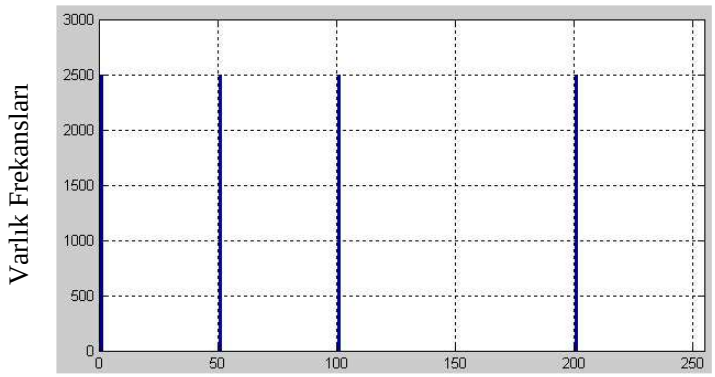
Bir sayısal video çerçevesi ya da imgenin histogramı, 0–255 arası renk ağırlık değerlerine ait kaç tane piksel olduğu konusunda bilgi verir. Örneğin bir imgeye ait histogram grafiği 255 değerine yakın bir bölgede yoğunlaşıyorsa o imgede beyaz rengin ve tonlarının yoğun olduğu düşünülür. Buna karşılık histogram 0 değerine yakın bölgede yoğunlaşıyorsa imgede siyah renk ve tonlarının yoğun olduğu yorumu yapılabilir.

Şekil 3.19'da 200×50 piksel boyutlarına sahip örnek bir gri tonlu imge ve bu imgeye ait histogram grafiği görülmektedir. İmgede toplam 10.000 adet piksel bulunmaktadır ve ilgili piksellerin 1/4'ü "0", 1/4'ü "50", 1/4'ü "100" ve kalan 1/4'ü ise "200" parlaklık değerlerine sahiptir. Özetle imgede 0, 50, 100, 200 parlaklık değerlerine ait 2500'er adet piksel yer almaktadır.



PPD: Piksel Parlaklık Değeri

(a)

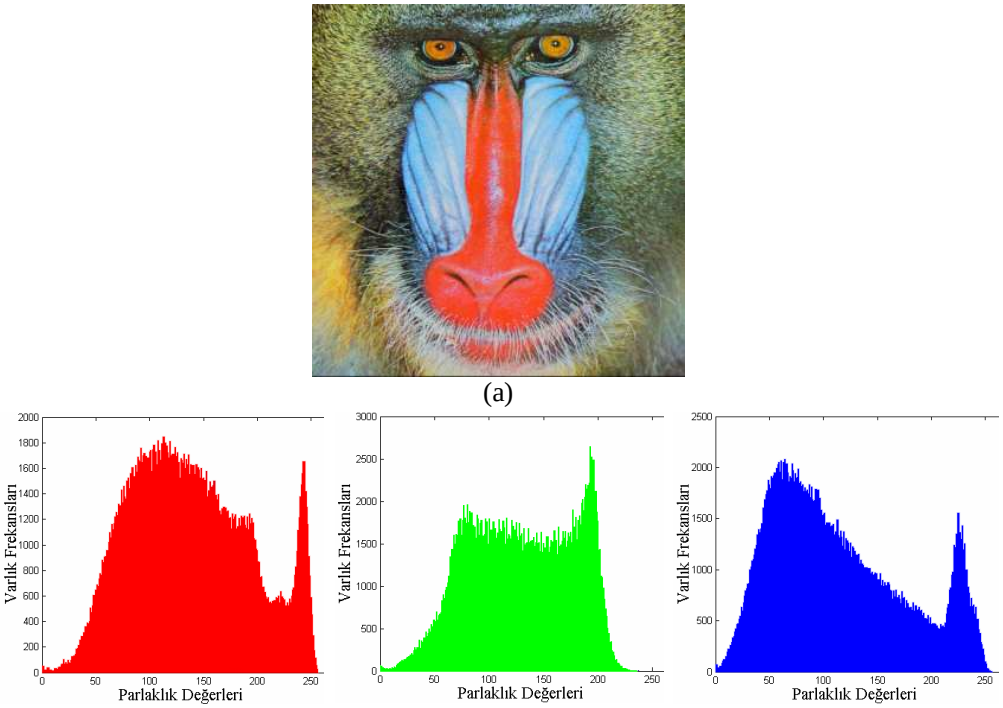


Parlaklık Değerleri

(b)

Şekil 3.19: 200×50 çözünürlüğe sahip gri tonlu bir imge (a) ve histogramı (b).

Renkli resimlere ait histogram grafikleri her bir renk değeri için elde edilmeli ve birlikte değerlendirilmelidir. Sayısal renkli resimlerde R, G, B, bileşenleri yer aldığından üç adet ayrı histogram grafiği (kırmızı, yeşil ve mavi histogramları) elde edilmelidir (Şekil 3.20). Adeta imgelerin ilk bakışta görülmeyen yüzü olarak nitelendirilebilecek histogramlar, akademisyenler için veri gizleme işlemlerinde kullanılan bir araç haline gelmiştir (Huang ve Fang, 2008, Hwang ve diğ., 2008, Lin ve diğ., 2008).



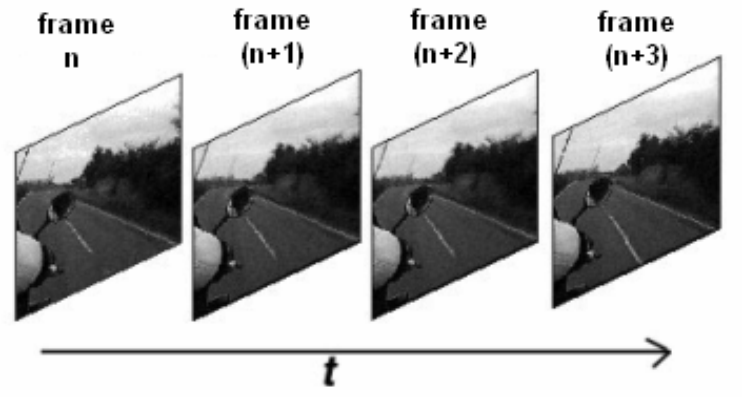
(a)

(b) (c) (d)

Şekil 3.20: RGB imge (a) ve R (b), G (c), B (d) histogramları.

3.6. Sayısal Video

Hareketsiz/sabit sayısal görüntülerin birim zamanda (1 saniyede) ardışık şekilde 25 kez veya üzerinde oynatılması ile elde edilen hareketli görüntülere sayısal video denir. Her bir sayısal görüntüye çerçeve (frame) denilir ve saniyedeki çerçeve sayısı fps (frame per second) kavramı ile ifade edilir (Çetin, 2008, Yalman ve Ertürk, 2009b) (Şekil 3.21).



Şekil 3.21: Bir videonun yapısı.

Hareketsiz resimlerin saniyede 25 kez veya daha fazla oynatılmasının nedeni, insan gözünün 25 Hz üzerindeki frekanslara hassasiyet gösterememesidir. Bu işlemin sonucunda insan gözü resimleri hareketli bir görüntü olarak algılamaktadır. Sayısal videonun oluşması için x, y ve z koordinatlar olmak üzere, bir ışık kaynağı (λ: dalga boyu), ışık kaynağının aydınlattığı bir nesne (E(x, y, z, λ)) ve nesnenin ışığı yansıtması (r(x, y, z, λ)) şartlarının sağlanması gerekir (Şekil 3.22). Elde edilen görüntünün matematiksel denklemi aşağıdaki şekilde ifade edilir.

$$c(x, y, z, \lambda) = E(x, y, z, \lambda) \times r(x, y, z, \lambda) \quad (3.6)$$

Şekil 3.22: Bir görüntünün oluşması.

İnsan gözünün algılama kapasitesi ile birlikte videolarda gösterilen sıralı imgelerin içeriği de çok önemlidir. Örneğin hareket ve renk değişiminin olmadığı bir zaman aralığında birim zamanda ekranda gösterilen çerçeve sayısının düşük olması algı açısından sorun oluşturmazken, sahne geçişlerinin ve renk bilgilerinin sürekli değiştiği zaman aralıklarında ise bu sayı 25 ve üzerinde olmalıdır.

Sayısal videolar sıkıştırılmış video ve sıkıştırılmamış video olarak iki farklı formata sahiptirler. Sıkıştırılmamış video formatı ilk kullanılan video tipidir ve en çok kullanılanı AVI (Audio–Video Interleave: Ses–Görüntü Birleşimi) dosyalardır. AVI formatındaki dosyalar; ses ve görüntünün birleştirilmesi ile oluşturulmuş videolardır. Bu formattaki videolar BMP formatındaki sıkıştırılmamış resim dosyalarının ardı sıra eklenmesi ile oluşturulur. Bu sebeple resim dosyaları üzerindeki kapasite hesabı, çözünürlük hesabı gibi işlemler AVI formatındaki videolar için de geçerlidir. Fakat bu dosyalar hafızada nispeten fazla yer kapladığından sıkıştırma teknikleri geliştirilmiş ve buna bağlı olarak da sıkıştırılmış video türleri geliştirilmiştir.

Sıkıştırılmış videolarda kullanılan tekniklerin sayısı gün geçtikçe gelişen sıkıştırma teknolojilerine paralel olarak artmaktadır (MPEG, H.264 (MPEG–4 AVC), WMV9, M–JPEG, SM4). Ancak, kayıplı sıkıştırma kullanılarak kodlanan video dosyalarının boyutunun küçülmesi ile birlikte, kalitesinin bozulması da söz konusudur (Tablo 3.3). Bu sebeple depolama ve iletim gereksinimi olmadığı müddetçe video dosyalarının sıkıştırılmamış şekilde saklanması daha olumlu bir yaklaşım olacaktır.

Tablo 3.3: Sayısal video standartları.

Video Standardı	**Çerçeve Boyutu Parlarlık (Luminance) ve Renklilik (Chrominance)**	**Bant Genişliği Gereksinimi (Sıkıştırılmamış)**
CIF (Common Interchange Format) (ITU–TS H.261)	Parlaklık (Y) : 352 × 288 Renklilik (U, V): 176 × 144	36 Mbps
QCIF (Quarter–CIF)	Parlaklık (Y) : 176 × 144 Renklilik (U, V): 176 × 144	18 Mbps
Super–CIF	Parlaklık (Y) : 704 × 576 Renklilik (U, V): 352 × 288	146 Mbps
VCR (Video Cassette Recording)– SIF Standard Interchange Format (MPEG–1 standardı için)	Parlaklık (Y) : 352 × 240 (NTSC için) Parlaklık (Y) : 352 × 288 (PAL/SECAM için) Renklilik (U, V): 176 × 120 veya 176 × 144	

3.7. Sonuç

Günümüzde sayısal imgeler ve imgeler dizisinden oluşan sayısal videolar çok çeşitli biçimlerde kaydedilmekte, saklanmakta ve iletilmektedir. Gelişen teknoloji ile birlikte hem dış ağ/iç ağ (internet/intranet) iletişim hızının artması, hem de depolama birimlerinin boyutlarının katlanarak büyümesi sonucu sıkıştırma gereksinimi azalmaktadır. Çünkü sıkıştırma işlemleri beraberinde görüntü kalitesinin düşürülmesi ve veri gizleme yöntemleri açısından gömü verisi kapasitesinin azalması anlamına gelmektedir. Tez çalışması kapsamında en kaliteli görüntü formatı olan ‘bmp’ uzantılı sayısal imgeler ve bu imgelerin kullanıldığı sayısal videolar olan AVI dosya tipi kullanılmıştır. Bu sayede hem kaliteli imgeler üzerinde çalışılmakta hem de gömü verilerinin yerleştirilmesi esnasında gereksiz kodlama yükünden kaçınılmaktadır.

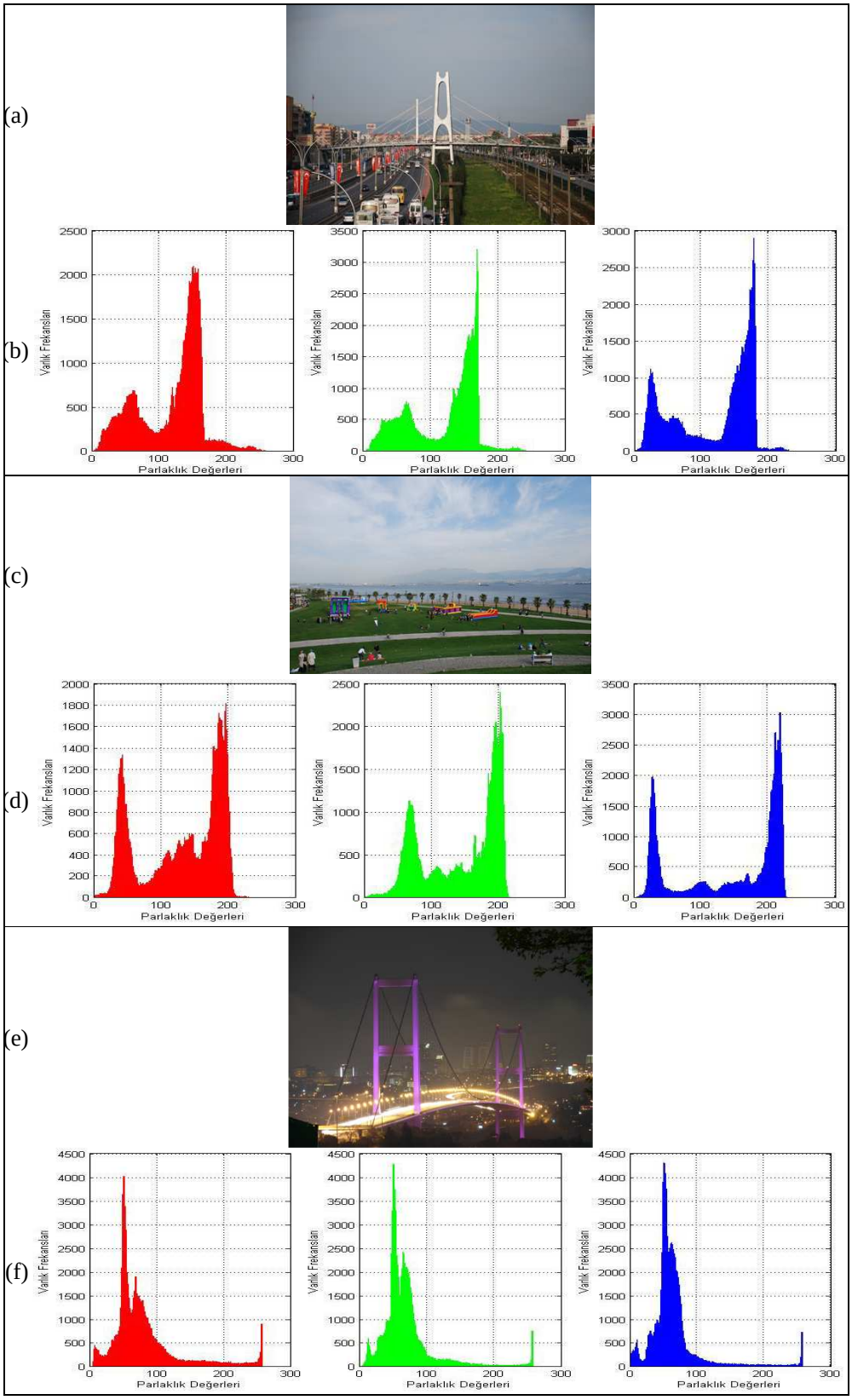
4. SAYISAL GÖRÜNTÜLER İÇİN HİSTOGRAM TEMELLİ VERİ GİZLEME YÖNTEMİ (HSV) VE UYGULAMA YAZILIMI (StegVid)

4.1. Giriş

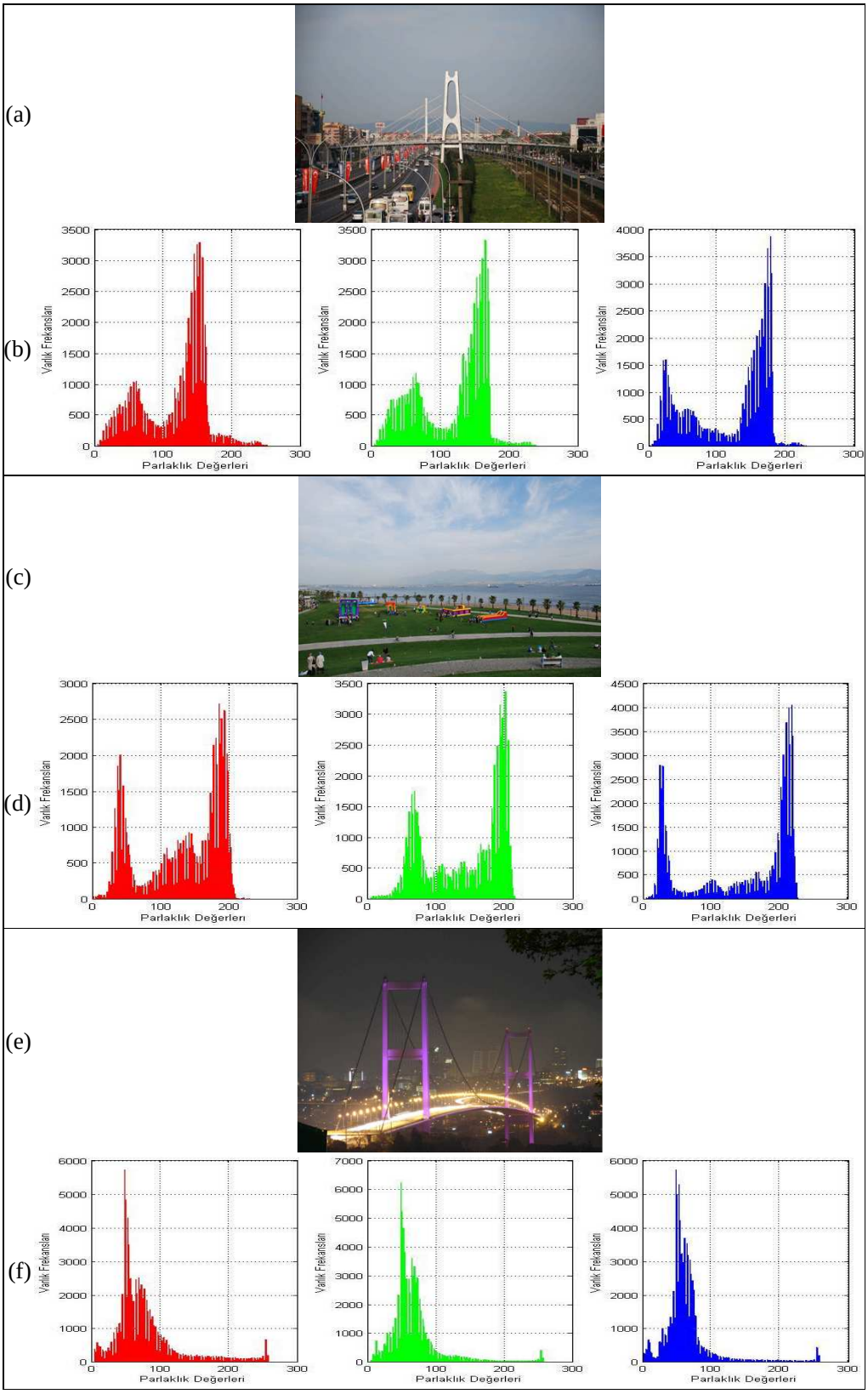
Histogram, bir işlem neticesinde elde edilen ölçüm sonuçlarının dağılımını gösteren grafiktir. İmge histogramı ise sayısal bir resmin parlaklık değerlerinin dağılımını gösterir. Tez çalışması kapsamında literatüre henüz girmemiş yeni bir yöntem olan HSV (**H**istogram based **S**teganography on **V**ideo) geliştirilmiş olup bir uygulama yazılımı (StegVid) ile de gerçeklenmiştir. Geliştirilen yöntemin temel amacı, sayısal görüntülere ait histogram değerlerini kullanarak veri gizleme işlemi gerçekleştirmektir. Tez çalışması kapsamında geliştirilen Histogram Temelli Veri Gizleme Yöntemi (HSV), en küçük değerlikli bitler kullanılarak yapılan veri gizleme tekniğini histogram işleme ile birleştirmektedir (Yalman ve Ertürk, 2009a, 2009c). Klasik eşleniklerine kıyasla, HSV başarımı nispeten daha iyi PSNR değerleri için daha fazla gömü verisi kapasitesi sağlamakla birlikte farklı başarım ölçütleri açısından da çok iyi sonuçlar vermektedir.

4.2. HSV Yönteminin Temel Çıkış Noktası: Sayısal İmge Histogramlarında Tarak Etkisi

Literatürde imge içerisine veri gömülmesi temelinde birçok uygulama geliştirilmiş olup, neredeyse tamamı İGS tarafından algılanamayacak bozulmalara sebep olmakta, böylece bilgi güvenliği sağlanmaktadır. Tez çalışması kapsamında yapılan araştırmalar doğal ortamdan elde edilen sayısal imgelerin (Şekil 4.1(a)–(c)–(e)) histogramlarının (Şekil 4.1(b)–(d)–(f)) düzenli bir dağılıma sahip olduğunu göstermiştir. Ancak İGS tarafından bozulmaların algılanamaz oluşu, imgenin veri taşıma ihtimalini ortadan kaldırmamaktadır. Şekil 4.2 (a)–(c)–(e)'de verilen LSB–2 bit ile kodlanmış imgelerin histogramlarındaki değişim açıkça görülmektedir.



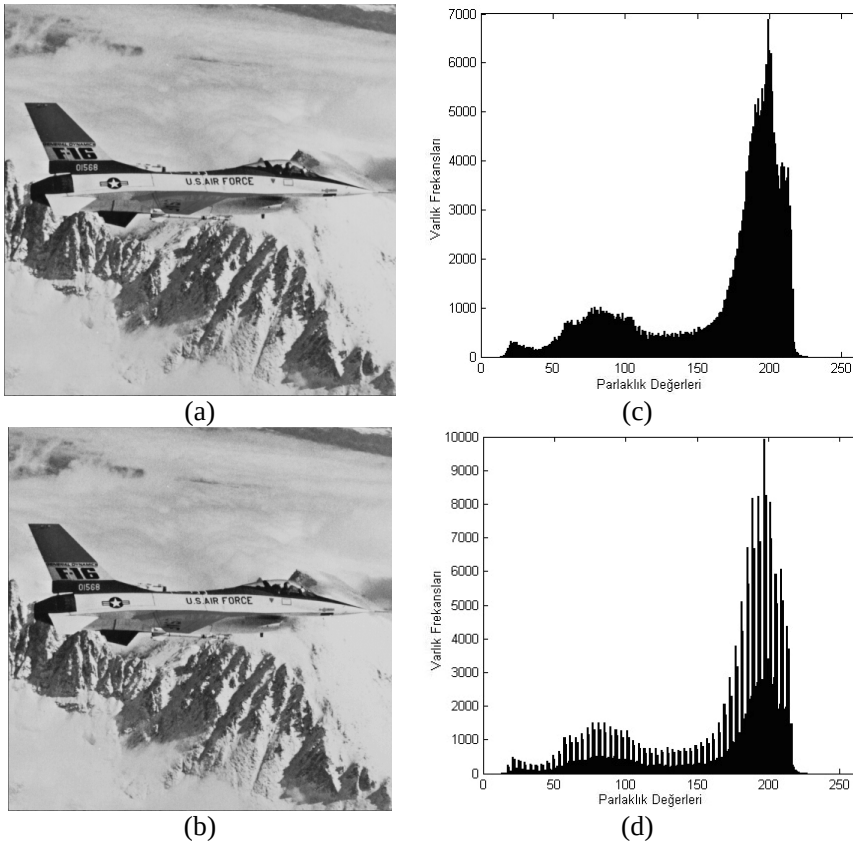
Şekil 4.1: Doğal imgeler (a–c–e) ve histogramlarına (b–d–f) ait örnekler.



Şekil 4.2: LSB–2 bit ile stego kodlu imgeler (Şekil 4.1 (a)–(c)–(e)) ve histogramları.

Şekil 4.2’de verilen imgelerdeki değişim İGS tarafından fark edilemese de, imgelere ait R, G, B histogramları bu durumu tersine çevirmektedir. İmge histogramlarındaki dengesiz dağılıma ve varlık frekanslarındaki ani değişimlere sebep olan etken tarak etkisi (comb effect) olarak adlandırılmaktadır (Yalman ve Ertürk, (2009a–c)). Bu sonuç, imgede istatistiksel olarak bir dengesizliğe işaret etmekte ve gizli veriyi taşıyan stego imgeler için önemli bir risk oluşturmaktadır.

Belirtilen etki sadece RGB imgelerde değil gri tonlu imgelerde de söz konusudur. Şekil 4.3(a)’da, orijinal görünümü ve histogramı (Şekil 4.3(c)) verilen imgenin, LSB–2 bit ile kodlandıktan sonraki görünümü (Şekil 4.3(b)) ve histogramı (Şekil 4.3(d)), tarak etkisinin varlığına işaret etmektedir. Burada dikkat edilmesi gereken iki sonuç söz konusudur. Birincisi, histogramlardaki tarağın dişlerini anımsatan görünüm iken ikincisi ise varlık frekansları ekseninin tepe nokta değerinin büyük oranda değişmesidir.



Şekil 4.3: Gri tonlu orijinal (a) ve stego imgelerin (b) histogramları (c–d).

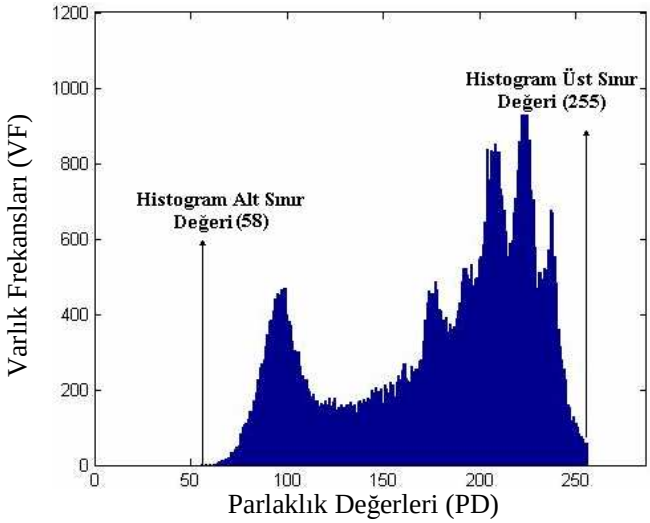
Sayısal imgelerin yanı sıra bit uzayında ifade edilen diğer sayısal verilerin (ses, metin vb.) tamamı için histogram elde edilebilmektedir. Veri gizleme yöntemlerinin olağan dışı bozulmalar oluşturması halinde, ifade edilen bu histogramlarda da tarak etkisinin oluşması kaçınılmazdır. Bu nedenle geliştirilen HSV yönteminin en az bir histograma sahip olan tüm sayısal verilerde kullanılabileceğini söylemek mümkündür.

Tarak etkisinin gömü verilerinin güvenliği açısından oluşturduğu riskler göz önünde bulundurulduğunda, özellikle görsel ve istatistiksel taramalara karşı gömülü verilerin şüphe uyandırmayan bir yapıda olması vazgeçilmez bir gerekliliktir. Bu sebeple imge histogramlarını temel alarak yeni bir veri gizleme yöntemi olan HSV geliştirilmiş olup, yönteme ait detaylar takip eden alt bölümlerde verilmektedir.

4.3. HSV Veri Gizleme İşlemleri

Veri gizleme işlemini yapan HSV ile histogram üzerinde İGS tarafından fark edilemeyecek değişiklikler oluşturulması hedeflenmektedir. Bu amaca yönelik olarak her piksel değerine (0–255) ait Varlık Frekansları (VF) dikkate alınarak veri gizleme işlemi yapılmaktadır.

Önerilen yöntemde, öncelikle imgeye ait histogram oluşturularak bu histograma ait Alt Sınır Değeri (ASD) ve Üst Sınır Değeri (ÜSD) tespit edilmektedir (Şekil 4.4). Böylece veri gizleme işleminin hangi Parlaklık Değerleri (PD) aralığında yapılacağı belirlenmekte ve imgede karşılığı olmayan parlaklık değerleri göz ardı edilmektedir. Bu sınır değerlerinden hareketle, veri gizleme işlemi aşağıda anlatıldığı şekilde gerçekleştirilmektedir.



Şekil 4.4: Bir imge histogramına ait alt ve üst sınır değerlerinin belirlenmesi.

Gizlenmek istenen ilk 3 bit değeri $(110)_2$ kabul edilsin. Verilerin gizleneceği imgenin R renk kanalının ise Şekil 4.4'teki gibi bir histograma sahip olduğu, alt sınır değerine ve sonraki birkaç değere ait varlık frekansları Şekil 4.5 ve Tablo 4.1'deki gibi kabul edilsin.

60	59	58	60	59	58	59
59	58	59	58	58	58	58
58	59	60	58	59	59	60
59	60	58	59	58	60	58
59	58	58	60	60	59	60
58	59	60	59	58	58	59
58	58	59	58	60	59	61

Şekil 4.5: İmgeye ait piksellerin sayısal değer haritasından bir kesit.

Tablo 4.1: İmge histogramına ait bazı sayısal değerler.

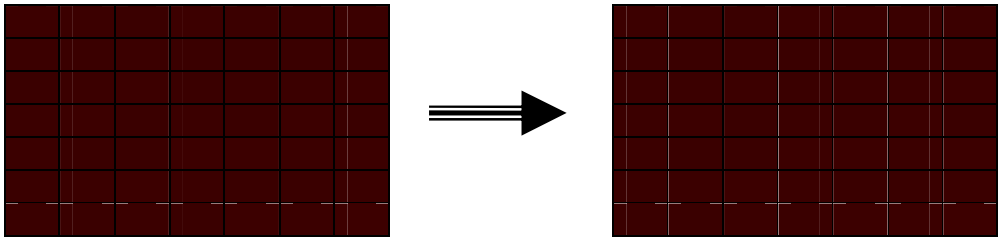
Piksel Parlaklık Değeri (PD)	58	59	60
Varlık Frekansları (VF)	20	17	11

HSV öncelikle gömü verisinin (yani $(110)_2$) ilk biti olan "1" değerini ele almaktadır. Öncelikle, histogram bilgileri kullanılarak alt sınır değerinin varlık frekansının 2 ile bölümünden kalan hesaplanmakta (VF(ASD) Mod2= 20 Mod2=0) ve gömü verisi ile

eşit olmadığından imge içerisindeki parlaklık değeri “58” olan piksellerden bir tanesi “59” olarak değiştirilmektedir. Böylece “58” parlaklık değerine ait varlık frekansı “19” olurken, “59”un varlık frekansı “18”e yükselmektedir. İlk gizli veri biti imge içerisine gömüldükten sonra histograma ait yeni değerler Şekil 4.6 ve Tablo 4.2’deki gibi olacaktır.

60	59	58	60	59	58	59
59	58	59	58	58	58	58
58	59	60	58	59	59	60
59	60	58	59	58	60	58
59	58	58	60	60	59	60
58	59	60	59	58	58	59
58	58	59	58	60	59	61

60	59	58	60	59	58	59
59	58	59	58	58	58	58
59	59	60	58	59	59	60
59	60	58	59	58	60	58
59	58	58	60	60	59	60
58	59	60	59	58	58	59
58	58	59	58	60	59	61



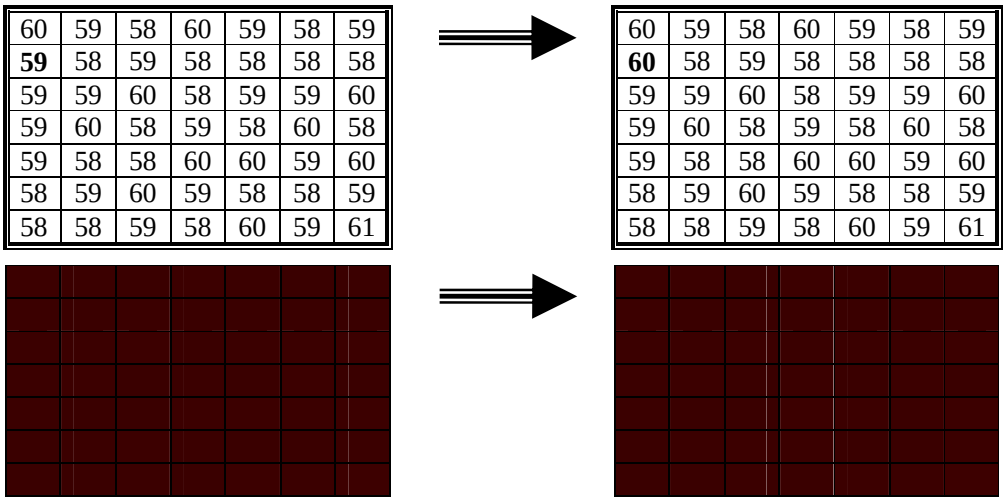
(a) (b)

Şekil 4.6: İlk gömü biti 1’in imgeye gömülmesinden önceki (a) ve sonraki (b) sayısal değer haritası ve piksel görünümleri.

Tablo 4.2: İmge histogramına ilk gömü biti “1” gizlendikten sonraki durum.

Piksel Parlaklık Değeri (PD)	58	59	60
Varlık Frekansları (VF)	19	18	11

Histogram bilgileri yenilendikten sonra, gömü verisinin ikinci biti “1” ele alınarak “59” parlaklık değerinin varlık frekansının 2’ye bölümünden kalan değer kontrol edilmektedir (VF(59) Mod2=18 Mod2 = 0). Elde edilen değer gömü verisi ile eşit olmadığından, imge içerisindeki parlaklık değeri “59” olan piksellerden bir tanesi “60” olarak değiştirilmektedir. Böylece “59” parlaklık değerine ait varlık frekansı “17” olurken, “60”ın varlık frekansı “12”ye yükselmektedir (Şekil 4.7 ve Tablo 4.3).



(a) (b)

Şekil 4.7: İkinci gömü biti "1"in imgeye gömülmesinden önceki (a) ve sonraki (b) sayısal değer haritası ve piksel görünümleri.

Tablo 4.3: İmge histogramına ikinci gömü biti "1" gizlendikten sonraki durum.

Piksel Parlaklık Değeri (PD)	58	59	60
Varlık Frekansları (VF)	19	17	12

Histogram bilgileri tekrar yenilendikten sonra, gömü verisinin üçüncü biti "0" ele alınarak "60" parlaklık değerinin varlık frekansının 2'ye bölümünden kalan değer kontrol edilmektedir (VF(60) Mod2=12 Mod2 = 0). Elde edilen değer gömü verisi ile farklılık göstermediğinden herhangi bir işlem yapılmamakta; dolayısıyla imgeye ait görünüm ve histogram değerleri, Şekil 4.7 ve Tablo 4.3'te olduğu gibi kalmaktadır.

Geliştirilen HSV yöntemi üç kanallı (RGB) imgelerde her kanal için histogramların ayrı ayrı hesaplanarak veri gizleme işlemine tabi tutulması ile gerçeklenmektedir. Histogram üst sınır değerinin "255" olduğu durumlarda, bu değere sahip olan piksellerden bir tanesinin (gömü bitinin değerine bağlı olarak) "256" olması gerekebilmektedir. Ancak her bir renk kanalı sekiz bit ile ifade edildiğinden "256" parlaklık değeri geçersiz bir değer olacaktır). Birçok yazılım bu durumda pikselin değerini 0 yapmakta ve tuz–biber etkisine sebep olmaktadır (Ni ve diğ., 2008). Bu

ihtimal göz önünde bulundurularak, önerilen yöntemde “255” parlaklık değerine sahip pikseller veri gizleme işleminde kullanılmamaktadır.

Sayısal ortamların kullanıldığı veri gizleme uygulamalarında gömü verisi miktarına ilişkin iki oran vardır. Bunlardan birincisi sabit veri gizleme oranı (CER: Constant Embedding Rate) iken diğeri ise değişken veri gizleme oranıdır (VER: Variable Embedding Rate) (Wu, 2001). Literatürde her iki oran temelinde geliştirilmiş olan yöntemler mevcuttur (Longmei ve diğ., 2003, Akar ve Varol, 2004).

İmgeye ait kanal sayısı K ve her bir kanalda bulunan parlaklık değeri sayısı ise P ile gösterilsin. Bu durumda HSV yöntemi açısından imgenin gömü verisi kapasitesi (C) Denklem 4.1'de görüldüğü şekilde ifade edilebilir.

$$C = \left(\sum_{i=1}^{K} P_i \right) - K \tag{4.1}$$

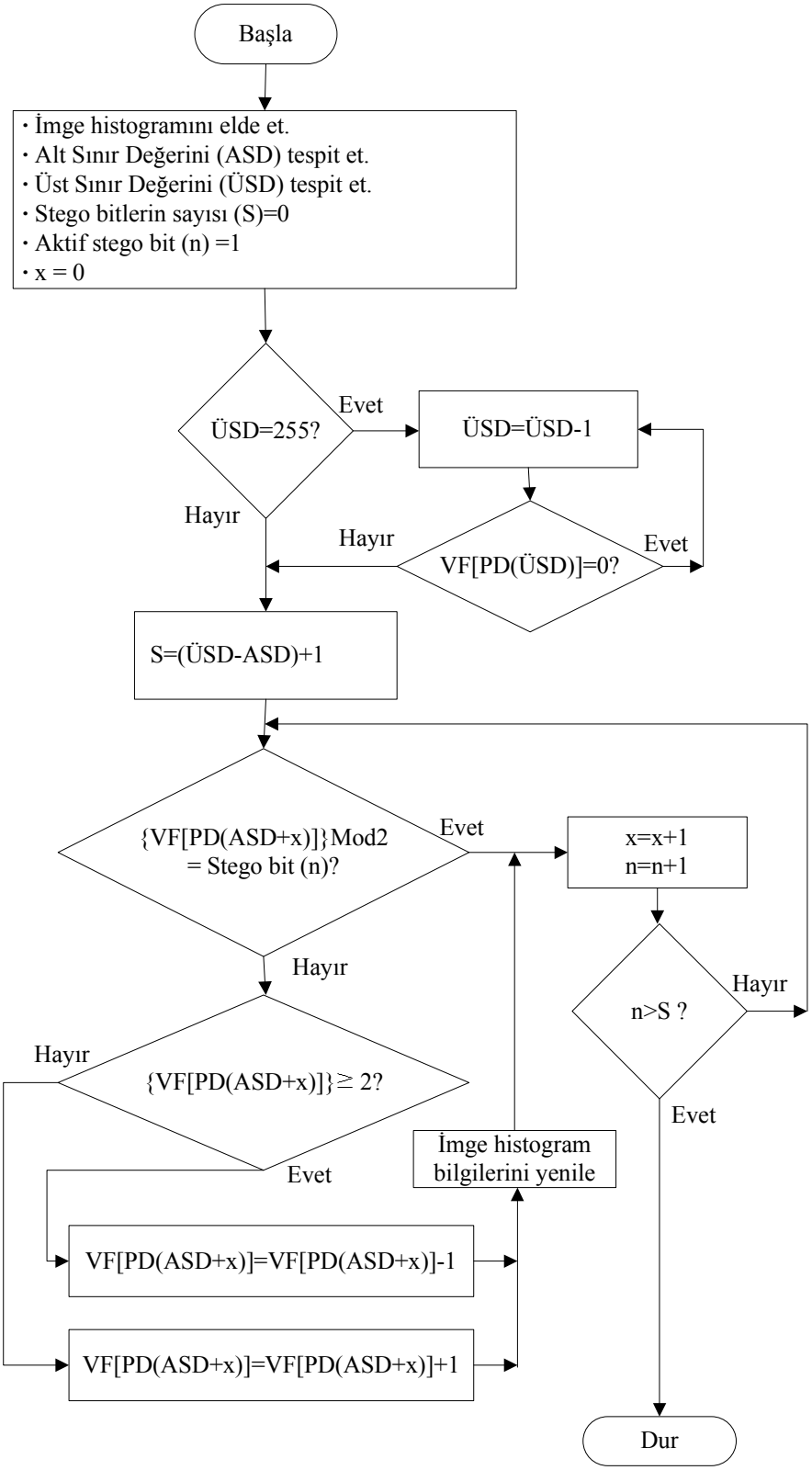
Denklem 4.1 göz önünde bulundurulduğunda, 3 kanallı ve her bir kanalında 256 adet parlaklık değerinin bulunduğu bir imgedeki gömü verisi kapasitesi:

$$C = \left(\sum_{i=1}^{3} P_i \right) - 3 = (256 + 256 + 256) - 3 = 765 \,\text{bit}$$

olarak hesaplanır. İmgenin N adet parçaya bölünmesi durumunda her bir parça için kapasite ayrı ayrı hesaplandıktan sonra toplam kapasiteye ulaşılır. Bu durumda kapasite Denklem 4.2'deki gibi ifade edilir.

$$C = \sum_{j=1}^{N} \left(\left(\sum_{i=1}^{K} P_i \right) - K \right) \tag{4.2}$$

Yukarıda verilen bilgilerden de görüleceği üzere önerilen HSV yöntemi, imgelere ait histogramlara bağımlı olarak gömü verilerini gizlediğinden VER temellidir. HSV veri gizleme işlemlerinin akış şeması Şekil 4.8’de verilmektedir.



Şekil 4.8: HSV veri gizleme akış şeması.

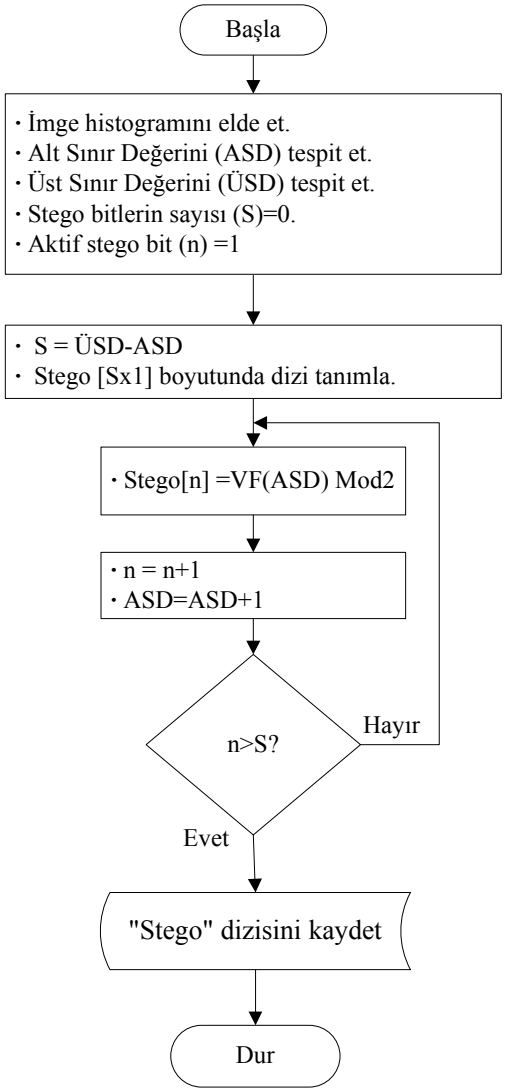
4.4. HSV Gömülü Gizli Veriyi Çıkartma İşlemleri

HSV yönteminde gizli verilerin çıkartılma işlemi, veri gizlemeye oranla çok daha basit şekilde gerçekleşmektedir. Öncelikle imgeye ait histogram değerleri elde edilmekte ve histogram sınırları tespit edilmektedir. Bu sınır değerleri dikkate alınarak parlaklık değerlerine ait varlık frekanslarının 2 ile bölümünden kalan değerler, gömü verisi olarak elde edilmektedir. Bu durumda histogram değerlerine ait bilgileri Tablo 4.3'teki gibi olan bir imgeye,

19 Mod2 = 1
17 Mod2 = 1
12 Mod2 = 0  $(110)_2$

işlemleri uygulanmakta ve $(110)_2$ değerinin imge içerisine gizlendiği tespit edilmektedir. Şekil 4.9'da gömülü/gizli veriyi çıkartma akış şeması verilmektedir.

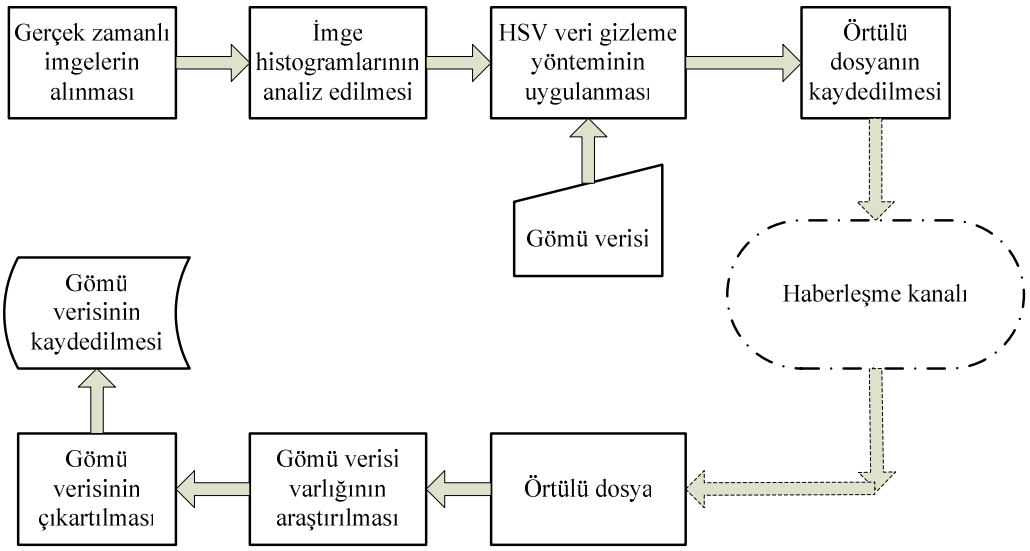
Gizli verinin gömülmesi ve gömülü gizli verinin çıkartılması aşamalarında, örneğin gizli verinin var olup olmadığı bilgisi ve gizli veri boyutu bilgisi gibi sayısal imzaların ya da başlık bilgilerinin taşıyıcı dosyalara eklenmesi zorunluluğu söz konusudur. Gömü verilerinin hareketli görüntülere gömülmesi sürecinde, HSV yönteminin bu zorunluluk için önerdiği çözümler takip eden alt bölümlerde detaylı şekilde anlatılmaktadır.



Şekil 4.9: HSV gömülü gizli veriyi çıkartma akış şeması.

4.5. HSV Yönteminin Gerçek Zamanlı Hareketli Görüntülerde Kullanımı

İmge histogramları temel alınarak verilerin gizlenmesini sağlayan HSV yöntemi ham video dosyalarında kullanılan sıralı imgelerde rahatlıkla kullanılabilmekte ve bu sayede gömü verisi kapasitesi de arttırılmaktadır (Şekil 4.10). İlgili sıralı imgelerin örneklerinin üçüncü kişilerin elinde olmasını engellemek amacıyla da web kamera kullanılarak güvenlik bir adım öteye taşınmaktadır.



Şekil 4.10: Veri gizleme/çıkartma işleminin genel blok şeması.

4.5.1. Gerçek zamanlı hareketli görüntü kayıtlarına HSV yöntemi ile veri gizlenmesi

Tez çalışması kapsamında geliştirilen HSV yöntemi tek bir imgeye uygulanabildiği gibi sıralı imgelere de uygulanabilmektedir. Bu sayede kapasite arttırılmakta, gerçek zamanlı sıralı imgelerin kullanılması ise güvenliği arttırıcı bir etken olmaktadır. Bir uygulama yazılımı (StegVid) ile de gerçeklenen bu yöntem saniyede 30 çerçevenin oynatıldığı “avi” dosyalar oluşturmaktadır. Ve İGS tarafından olağandışı bir durumun oluştuğunun fark edilmesi imkânsız hale getirilmektedir. Takip eden bölümlerde de belirtildiği gibi istatistiksel olarak da fark edilemeyen bir yöntemle veri gizleme işlemleri gerçekleştirildiğinden üçüncü kişilerde şüphe uyandırmayan bir haberleşme ortamı oluşturulmaktadır. Bu yönleri ile HSV, literatürdeki birçok eşleniğine oranla daha iyi sonuçlar vermektedir.

HSV hareketli görüntü kayıtları içerisine gizli verinin varlığına işaret eden, gömü verisinin boyutu ve tipine göre farklılık gösteren bir başlık bilgisini yerleştirmektedir. Eğer gömü verisi bir dosya ise başlık bilgisi Tablo 4.4’teki gibi oluşturulmaktadır.

Tablo 4.4: Gömü verisinin dosya olması durumunda başlık bilgisinin oluşturulması.

Başlık bilgisindeki sıra	**Gömülen bilgi**
1–24. bit	Gömü dosyası var bilgisi. (110011001100110011001100) olarak belirlenmiştir.
25–48. bit	Gömü dosyasının boyut (16 MB'a kadar) bilgisi.
49–72. bit	Gömü dosyasının uzantı bilgisi.
73– n. bit	Gömü dosyası bitleri (n: Gömü verisinin boyutuna bağlı olarak değişmektedir.)

Başlık bilgisi, gömü verisini 72 bit arttırmakta olup bu durum gömü verisi kapasitesi açısından olumsuz bir durum teşkil etmemektedir. Yukarıda verilen bilgilerden hareketle 2,5 MB (Mega Bayt) boyutundaki ".doc" uzantılı bir dosyaya ait başlık bilgisi Tablo 4.5'teki gibi oluşturulmaktadır.

Tablo 4.5: Örnek bir gömü dosyasına ait başlık bilgisinin hazırlanması.

<table>
<tr><th colspan="4">Hazırlanan veri tipi</th><th>Hazırlanan verinin bit karşılığı</th></tr>
<tr><td colspan="4">Gömü dosyası var bilgisi</td><td>110011001100110011001100</td></tr>
<tr><td colspan="4">Dosya boyutu= 2,5 MB = 2621440 bayt</td><td>00101000000000000000000</td></tr>
<tr><td>Dosya uzantısı</td><td>d</td><td>o</td><td>c</td><td rowspan="3">011001000110111101100011</td></tr>
<tr><td>ASCII kod karşılığı</td><td>100</td><td>111</td><td>99</td></tr>
<tr><td>Bit karşılıkları</td><td>01100100</td><td>01101111</td><td>01100011</td></tr>
<tr><th colspan="5">Başlık bilgisi (72 bit)</th></tr>
<tr><td colspan="5">110011001100110011001100001010000000000000000000001100100011011110110001 1</td></tr>
</table>

Yukarıda verilen örnek ile birlikte farklı dosya tiplerinin gömülmesi de sağlanabilmektedir (txt, png, exe, jpg, zip, rar vb.). Gömü verilerinin sıkıştırılması ve şifrelenmesi ile elde edilecek ".rar" veya ".zip" uzantılı dosyaların gizli haberleşmede kullanımı, güvenliği çok olumlu yönde arttıracaktır.

Uygulama yazılımının kullanılması esnasında kullanıcı tarafından oluşturulan karakter dizisinin (metin) gömü verisi olarak belirlenmesi durumunda ise başlık bilgisi Tablo 4.6'da belirtildiği şekilde oluşturulmaktadır.

Tablo 4.6: Gömü verisinin metin olması durumunda başlık bilgisinin oluşturulması.

Başlık bilgisindeki sıra	Gömülen bilgi
1–24. bit	Gömü metni var bilgisi (101010101010101010101010) olarak belirlenmiştir.
25–40. bit	Gömü metninin boyut (65536 karaktere kadar) bilgisi.
41–n. bit	Gömü metni bitleri. (n: Gömü metninin uzunluğuna bağlı olarak değişmektedir.)

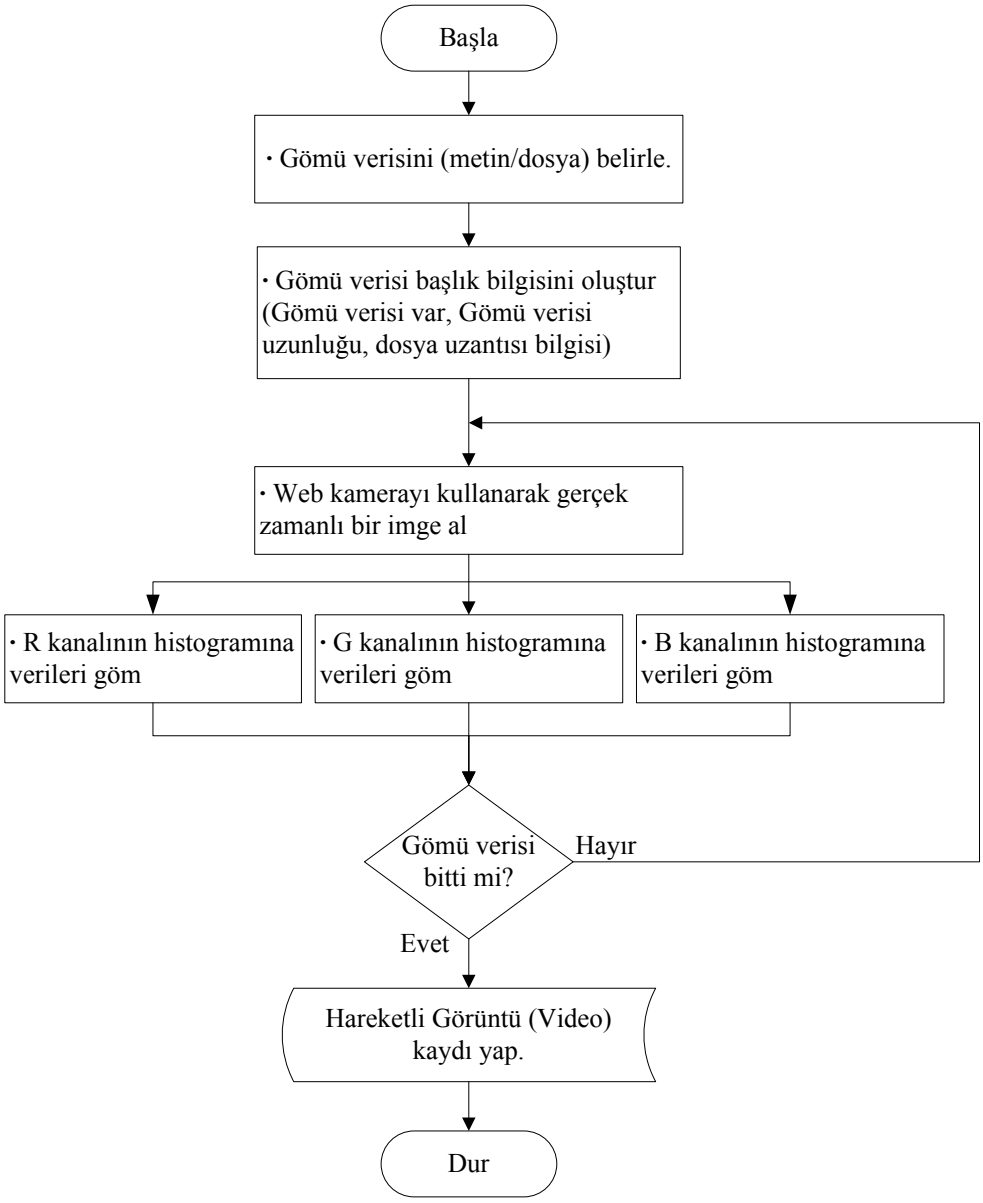
Yukarıda verilen bilgilerden hareketle 3200 karakterlik bir metin gömülmek istendiğinde başlık bilgisi Tablo 4.7'deki gibi oluşturulmaktadır.

Tablo 4.7: Örnek bir gömü metnine ait başlık bilgisinin hazırlanması.

Hazırlanan veri tipi	Hazırlanan verinin bit karşılığı
Gömü metni var bilgisi	101010101010101010101010
Gömü metni boyutu= 3200 karakter = 3200 bayt (8 bit ASCII kod tablosu referans alınmaktadır.)	0000110010000000
Başlık bilgisi (40 bit)	
101010101010101010101010 0000110010000000	

Oluşturulan başlık bilgisinin imge histogramına gömülmesinin ardından gömü dosyasının/metninin bitleri sırasıyla R, G ve B kanallarının histogramlarına gizlenmekte ve aktif işlem gören imgenin kapasitesi yeterli olmadığı sürece web kamera aracılığı ile yeni imgeler alınarak veri gizleme işlemine devam edilmektedir (Şekil 4.11). Gömü verisinin varlığına işaret eden 24 bitlik anahtarlar rasgele belirlenmiş olup, algoritmanın esnek yapısı sayesinde değiştirilebilmektedir. Bununla birlikte gömü dosyası boyutu ve gömü metni boyutu için ayrılan bit sayıları da HSV ve StegVid'in esnek yapısı sayesinde değiştirilebilmektedir.

Kablolu ya da kablosuz haberleşme ortamında iletilecek olan gömülü videolara ait çerçevelerde meydana gelecek herhangi bir kayıp gömü verilerinin güvenliği açısından olumsuzluk teşkil edecektir. Ancak OSI (Open System Interconnection) referans modelinin 4. katmanı olan ulaşım katmanı (transport layer) kayıpları telafi edeceğinden, olması muhtemel olan bu sorun üzerinde durulmamaktadır.

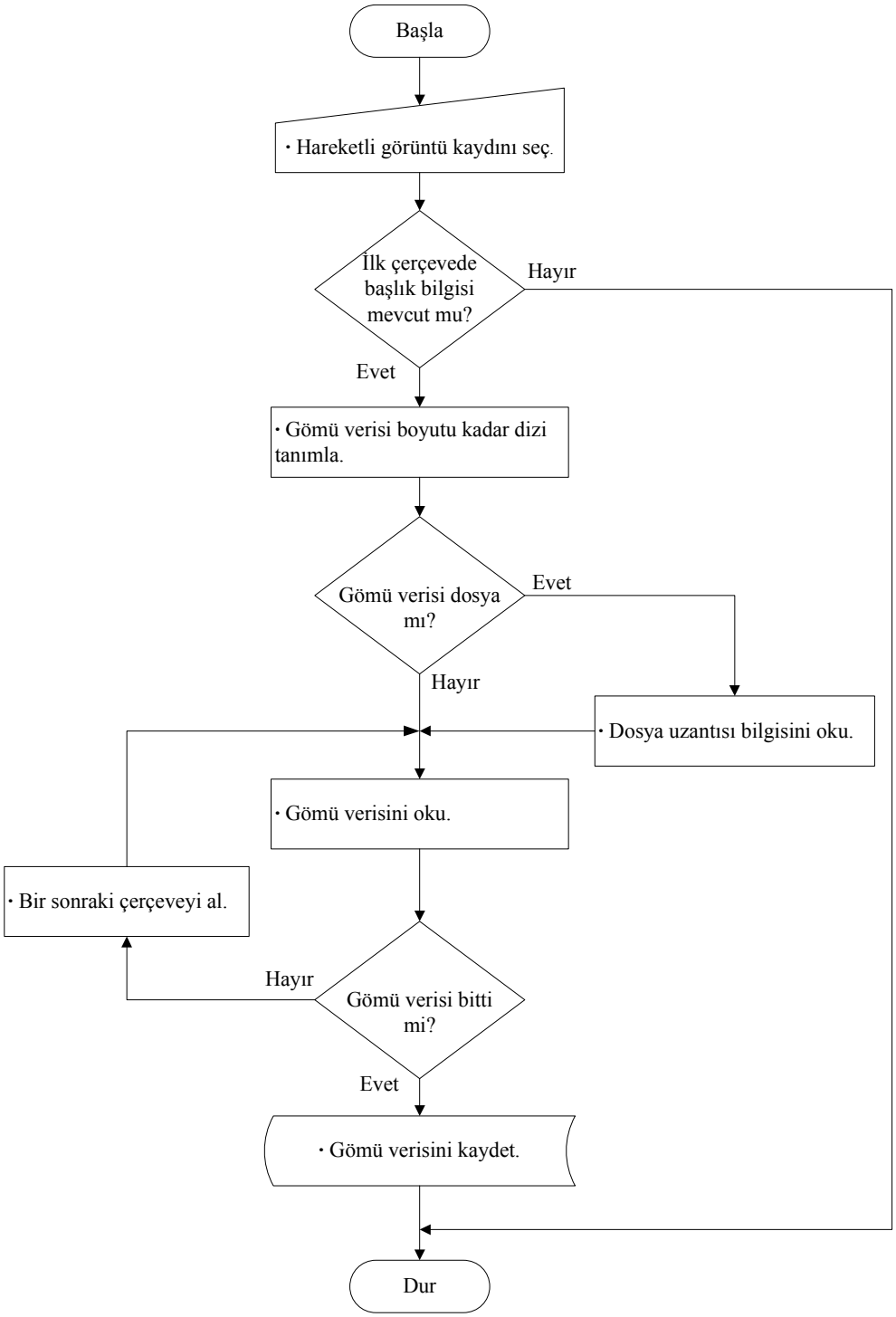


Şekil 4.11: Gerçek zamanlı hareketli görüntü kayıtlarına HSV yöntemi ile veri gizleme akış şeması.

4.5.2. HSV çıktısı hareketli görüntü kayıtlarından gömü verilerinin çıkartılması

Gömü verilerinin çıkartılması sürecinde ilk olarak videoya ait ilk çerçevede gömü verisinin varlığına ilişkin araştırma yapılmaktadır. Gömü dosyası varlığının tespit edilmesi durumunda, ilgili gömü verileri sıralı çerçevelerden elde edilerek belirtilen

dosya ya da metin olarak kaydedilmektedir. Gömü verisinin metin olması durumunda ilgili metin sıralı video çerçevelerinden okunarak bir “txt” dosyaya kaydedilmekte ve gizli mesaj elde edilmektedir (Şekil 4.12).



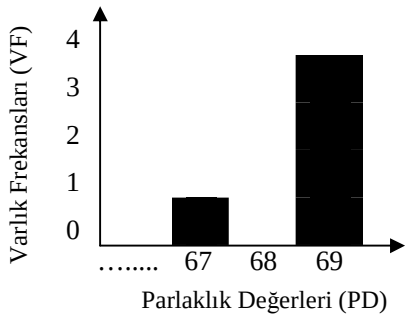
Şekil 4.12: Hareketli görüntü kayıtlarından gömülü gizli veri çıkartma akış şeması.

4.6. Sayısal Görüntü Histogramlarındaki Muhtemel Özel Durumların HSV Yönteminde Çözümleri

Yapılan deneysel çalışmalar gerçek zamanlı olarak web kamera aracılığıyla elde edilen imgelerin histogramlarındaki bazı özel durumların çözümlenmesinin zorunlu olduğunu ortaya koymuştur. HSV yönteminin uygulanma sürecinde bu özel durumlar göz ardı edildiği takdirde gömü verisinin sağlıklı şekilde gizlenmesi gerçekleşmemekte ve bir takım sorunlar oluşmaktadır. Bu özel durumlar ve önerilen çözüm yöntemleri aşağıda örnekler üzerinde açıklanmaktadır.

Özel Durum I:

İlk olarak bir imgenin histogramına ait belirli bir bölümün Şekil 4.13'deki gibi olduğu ve gömü verisi olarak $(01)_2$ gömüleceği varsayılsın.

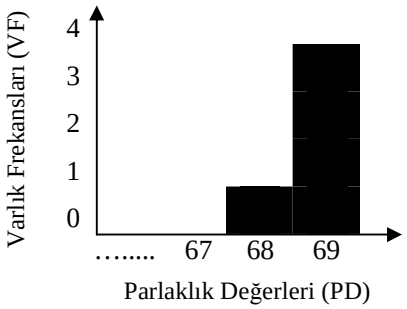


Şekil 4.13: Özel durum I'e ait örnek histogram görünümü.

HSV öncelikle VF[PD(67)]'ye, gömü verisi "0" değerini gizlemek üzere işlem yapacaktır.

VF[PD(67)] Mod2= 1 Mod2 = 1 (4.3)

olduğundan; yöntemin temel ilkesi gereği, imge içerisindeki parlaklık değeri "67" olan tek pikselin değeri "68" olarak değiştirilmesi gerekir. Dolayısı ile imge histogramı Şekil 4.14'teki gibi olur.

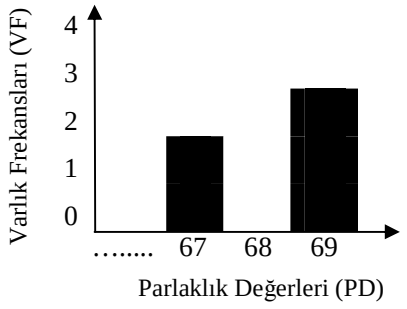


Şekil 4.14: Özel durum I'e ait gömü verisi taşıyan histogram görünümü.

HSV gömü verisini elde etme sürecinde, VF değeri "0" olan tüm parlaklık değerlerini ilgili işlemlerin dışında tutmaktadır. Buna rağmen Şekil 4.14'te görülen yeni histogramda hem VF[PD(67)] değeri "0" olmuş, hem de değişime uğramaması gereken VF[PD(68)] ise "1" olarak değişmiştir. Gelinen bu noktada, bahsedilen sorunu ortadan kaldırmak için yöntemin gerçeklenmesi aşamasında, ilgili durum göz önünde bulundurularak yukarıdaki örnek özelinde, aşağıdaki adımlar uygulanır:

Adım 1: PD(X)> 67 ve VF[PD(X)] ≥ 2 koşulunu sağlayan ilk "X" değeri belirlenir.
Adım 2: İmge içerisindeki parlaklık değeri "X" olan piksellerden birinin değeri "67" olarak değiştirilir.

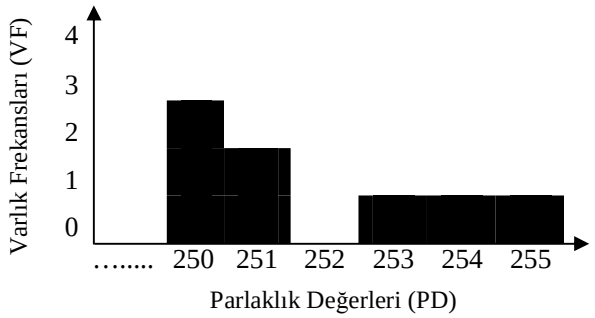
Şekil 4.13'te verilen histogram göz önünde bulundurulduğuna, ilgili şartları sağlayan X değerinin "69" olduğu kolaylıkla tespit edilebilir. Bu noktadan hareketle, imgedeki PD(69) olan piksellerden biri PD(67) olarak değiştirildiğinde, yeni histogram HSV yönteminde belirlenen kurallara uygun şekilde oluşacak ve gömü verisi sorunsuz şekilde gizlenecektir (Şekil 4.15).



Şekil 4.15: Özel durum I'in çözümlenmesi ile oluşan yeni histogram görünümü.

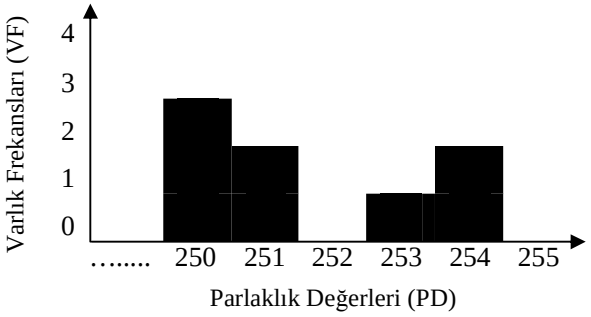
Özel durum II:

Bir imgenin histogramına ait belirli bir bölümün Şekil 4.16'daki gibi olduğu, VF[PD(250)], VF[PD(251)] ve VF[PD(253)] değerlerine gömü verilerinin gizlenmiş olduğu, veri gizleme işlem sırasının VF[PD(254)]'de olduğu varsayılsın. Bu durumda ilgili VF değerlerine gizlenen gömü bitlerinin sırası ile "1", "0" ve "1" olduğu söylenebilir.



Şekil 4.16: Özel durum II'ye ait örnek histogram görünümü.

VF[PD(254)]'e, "0" değerinin gizlenmek istenmesi durumunda, yukarıda detayları verilen özel durum oluşacak ve sorunun aşılması için imge içerisindeki parlaklık değeri "255" olan bir pikselin değeri, "254" yapılarak çözüm sağlanmış olacaktır (Şekil 4.17).



Şekil 4.17: VF[PD(254)]'e "0" gizlendikten sonraki histogram görünümü.

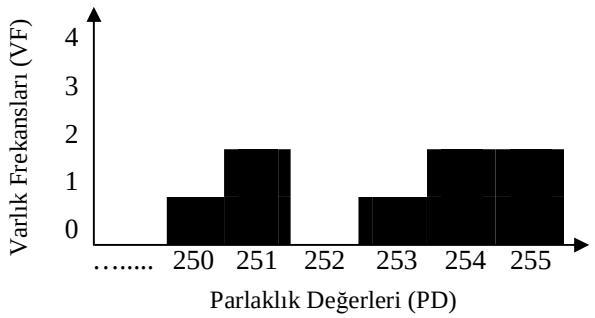
Ancak bu çözüm yeni bir sorunun ortaya çıkmasına sebep olmaktadır. Çünkü HSV, gerektiğinde kullanmak üzere VF[PD(X)]>0 şartını sağlayan en büyük X değerini tespit ederek bu değere Üst Sınır Değeri (ÜSD) adını vermektedir. ÜSD gömü verisi

elde etme sürecinde de tespit edilerek işleme alınmamaktadır (çünkü bu değer gömü verisi içermemektedir). Şekil 4.17'de oluşan yeni histogram ele alındığında ÜSD değerinin 254 olduğu görülecektir. Yukarıdaki bilgilerden hareketle VF[PD(254)]'ün işleme alınmaması sonucunda, gömü verisinin elde edilmesinde 1 bitlik hata yapılacağı söylenebilir.

Sonuç olarak; ortaya çıkan problem ÜSD'nin imge histogramından kaybolması durumudur. Bu durumun ortaya çıkmaması için Şekil 4.16 dikkate alındığında aşağıdaki adımların uygulanması önerilmektedir:

Adım 1: PD(X)< 254 ve VF[PD(X)]>2 şartını sağlayan ilk "X" değeri belirlenir.
Adım 2: İmge içerisindeki parlaklık değeri "X" olan piksellerden 1 tanesinin değeri "ÜSD" olarak değiştirilir (bu örnek için "255" yapılır).
Adım 3: İmge içerisindeki parlaklık değeri "X" olan piksellerden 1 tanesinin değeri "254" olarak değiştirilir.

Yukarıdaki adımlar uygulandığında, hem varlık frekanslarına gizlenen gömü verileri kayba uğramayacak hem de ÜSD değeri histogramdan kaybolmayacaktır (Şekil 4.18).



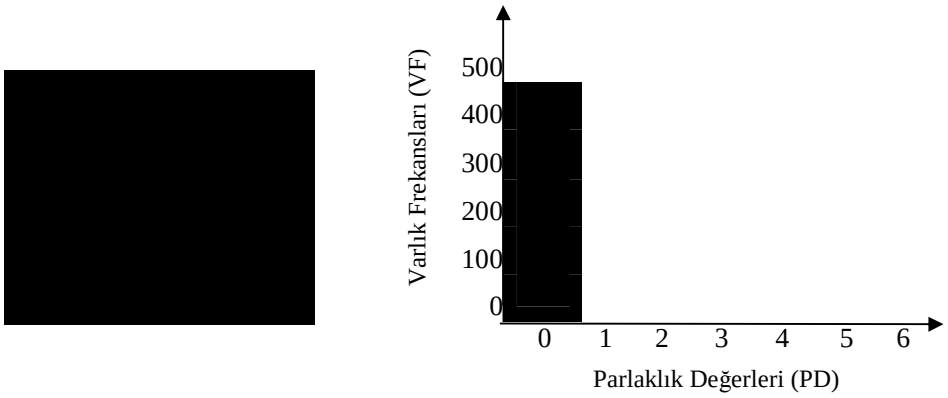
Şekil 4.18: Özel durum II'nin çözümlenmesi ile oluşan yeni histogram görünümü.

Özel durum III:

Geliştirilen yöntemin histogram temelinde işlem yapmasının getirdiği avantajlar ile birlikte bazı dezavantajları da bulunmaktadır. Literatürde sunulan birçok yöntem resim çözünürlüğüne bağlı olarak gömü verisi kapasitesini garanti etmektedirler.

Ancak sunulan çalışmada bu durum imge içerisinde bulunan piksel parlaklık değerlerinin çeşitliliğine bağlı olarak değişmektedir.

Örneğin tamamen siyah ya da tamamen beyaz renklerden oluşan bir imgeye gömülecek veri miktarı oldukça küçük seviyelerde kalacaktır (Şekil 4.19). Ancak doğal ortamda böyle bir imgenin oluşması ve bu tür imgelere veri gömülmesi ihtimalinin düşük oluşu ortaya çıkan dezavantajın büyük bir sorun oluşturmaması anlamına gelmektedir. Gömü verisi kapasitesini arttırmak adına histogram yayma tekniklerinin kullanılması bu tip durumlarda kullanılabilecek bir yöntemdir.



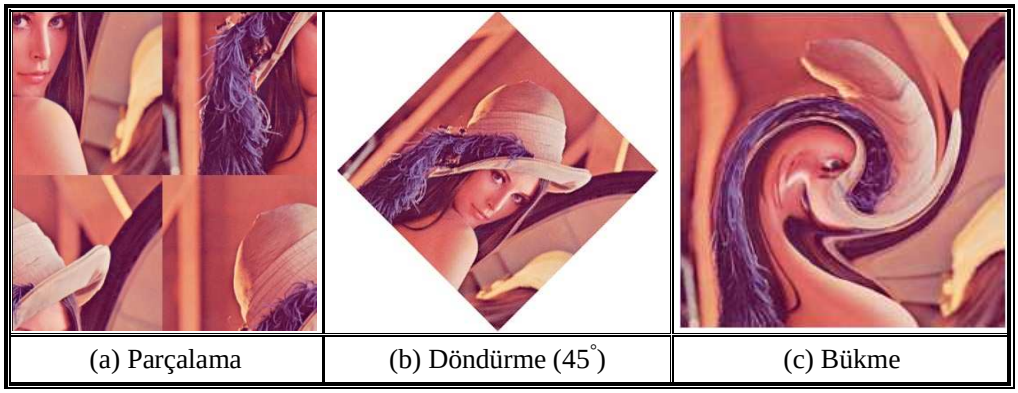
(a) (b)

Şekil 4.19: Tek renkten oluşan imge (a) ve histogramı (b).

4.7. Sayısal İmgelere Yapılan Geometrik Ataklara Karşı HSV Yönteminin Dayanıklılığı

Özellikle damgalama işlemine tabi tutulan veya gömü verisi taşıma ihtimali yüksek görülen sayısal imgelere sıkıştırma, kırpma, bükme, vb. gibi ataklar gerçekleştirilir. Söz konusu atakların yapılmasındaki amaç gömü verisini elde etmek değil, ilgili verileri yok etmektir. Piksellerin imgedeki konumu ile ilgili ataklara geometrik ataklar denir ve çoğunlukla imge histogramını değiştirmezler. Geometrik ataklar parçalama, döndürme, bükme, vb. şekillerde uygulanabilir (Şekil 4.20).

Bir imge histogramı, piksel parlaklık değerlerine ait varlık frekansları ile ilgilenirken, piksellerin imge içerisindeki konumları ile ilgilenmez. Bu, söz konusu olan sayısal imgeye ait piksellerinin rasgele dağıtılması durumunda bile histogramın değişmeyeceği anlamına gelmektedir. Sonuç olarak, imge histogramını referans alarak veri gizleme işlemi yapan HSV yönteminin geometrik ataklara karşı dayanıklı olduğu söylenebilir.



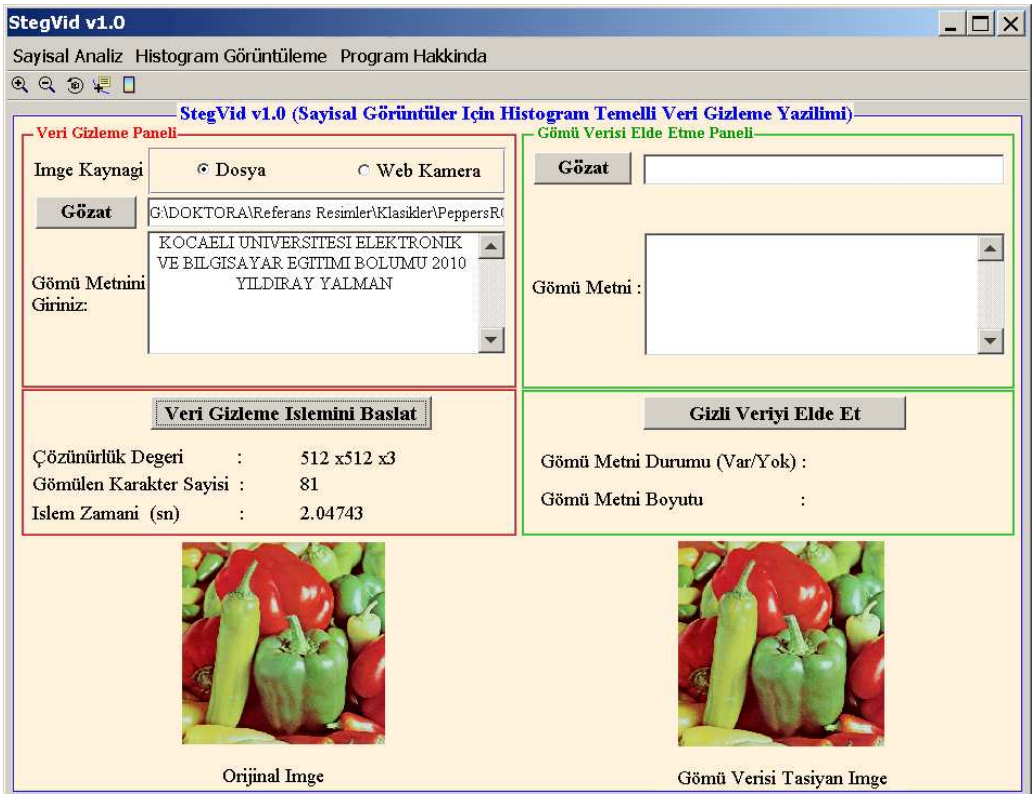
(a) Parçalama | (b) Döndürme (45°) | (c) Bükme

Şekil 4.20: Çeşitli geometrik atak örnekleri.

İmgelere üçüncü kişiler tarafından çeşitli atakların yapılması ve yöntemlerin bu ataklara karşı dayanıklılığı (robustness) damgalama bilimi ile yakından ilişkili olup steganografi uygulamalarında sıklıkla ön plana çıkan bir konu değildir. Ancak tez çalışması kapsamında geliştirilen HSV yönteminin bu yönüne de vurgu yapılarak damgalama uygulamalarında da kullanılabileceği öngörülmektedir.

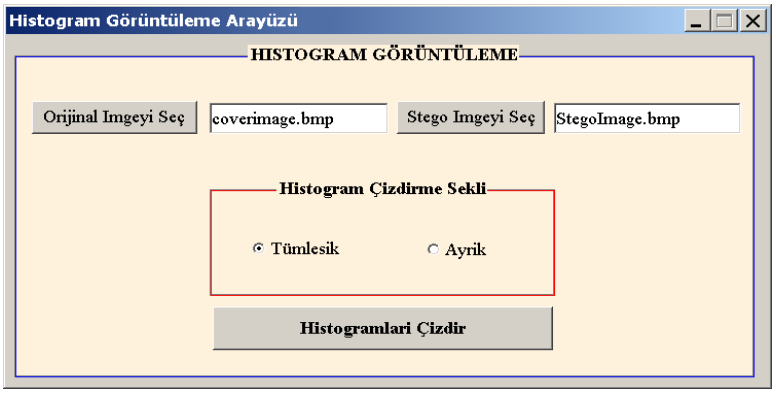
4.8. Sayısal İmgelere ve Videolara HSV Yöntemi İle Veri Gizleme Yazılımı: StegVid

Tez çalışması kapsamında geliştirilen histogram temelli veri gizleme yöntemi HSV için uygulama yazılımı StegVid geliştirilmiştir. StegVid v1.0 olarak adlandırılan ilk yazılım, tek bir imgeye HSV yöntemini uygulayarak veri gizleme işlemini yapmaktadır (Şekil 4.21).

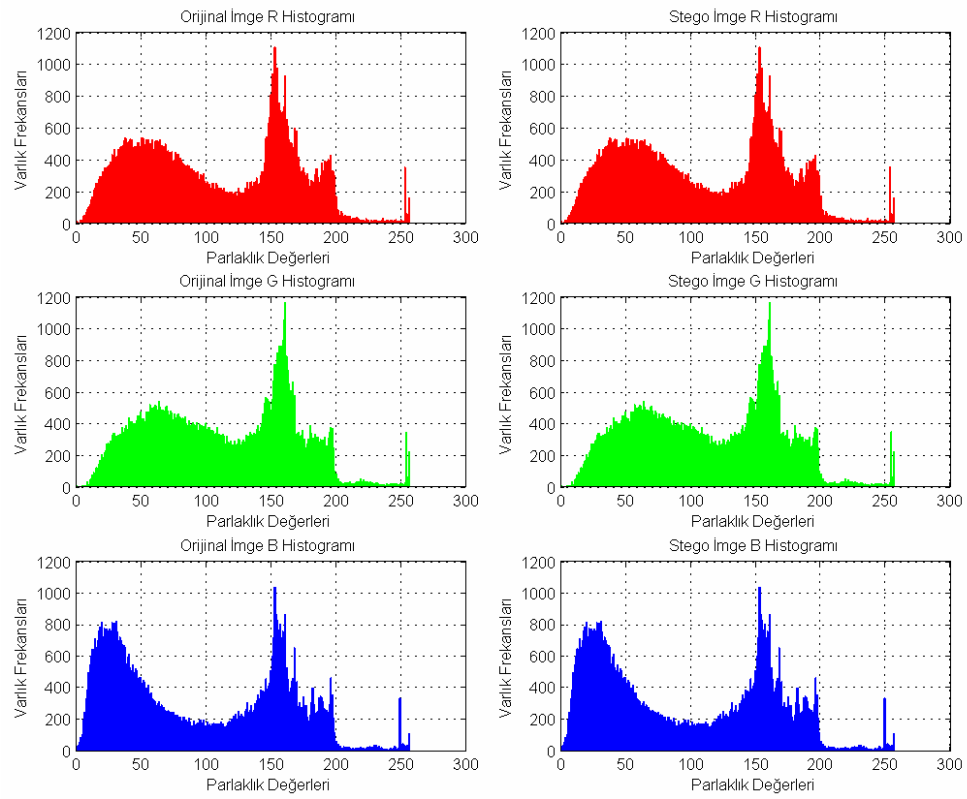


Şekil 4.21: Sayısal imgelere HSV'nin uygulanmasını sağlayan uygulama yazılımı StegVid v1.0 arayüzü.

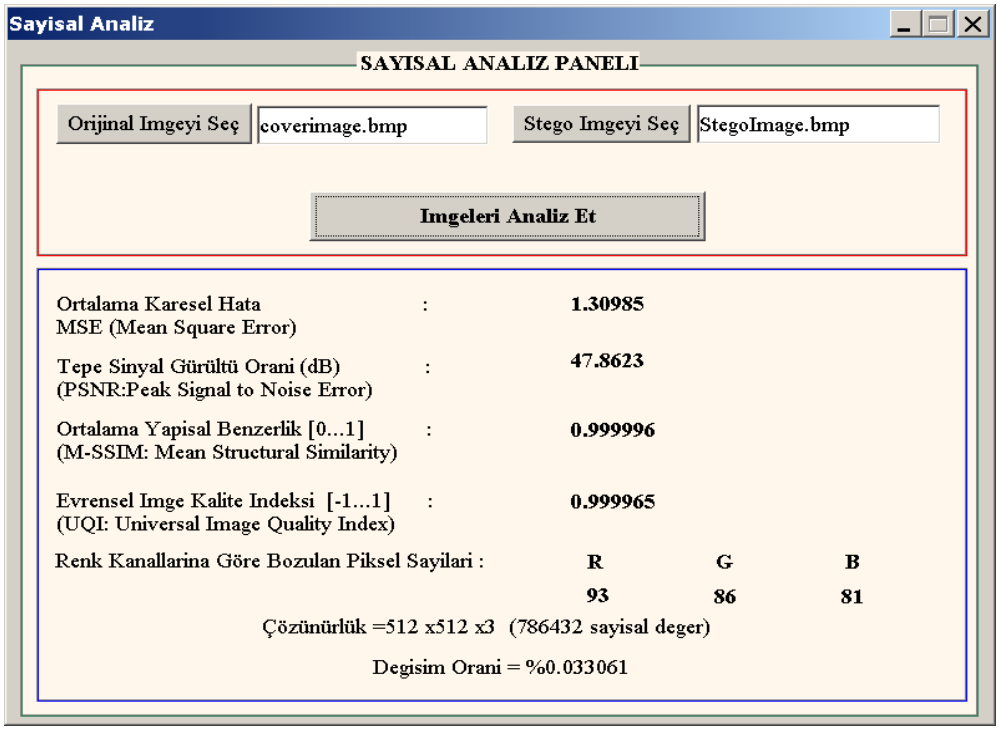
StegVid v1.0 aynı zamanda çok farklı başarım analizlerinin yapılmasına (MSE, PSNR, M–SSIM, UQI, Gömü verisi kapasitesi, Bozulma oranı, Histogram analizi, Görsel analiz) imkân vererek görsel ve sayısal sonuçları kapsamlı şekilde sunmaktadır (Şekil 4.22, Şekil 4.23 ve Şekil 4.24). Bununla birlikte StegVid'in kullanım alanının genişletilmesi için, benzer uygulamalardan elde edilen imgelerin başarım analizleri de yapılabilmektedir.



Şekil 4.22: İmge histogramlarının görüntülenmesini sağlayan pencere.

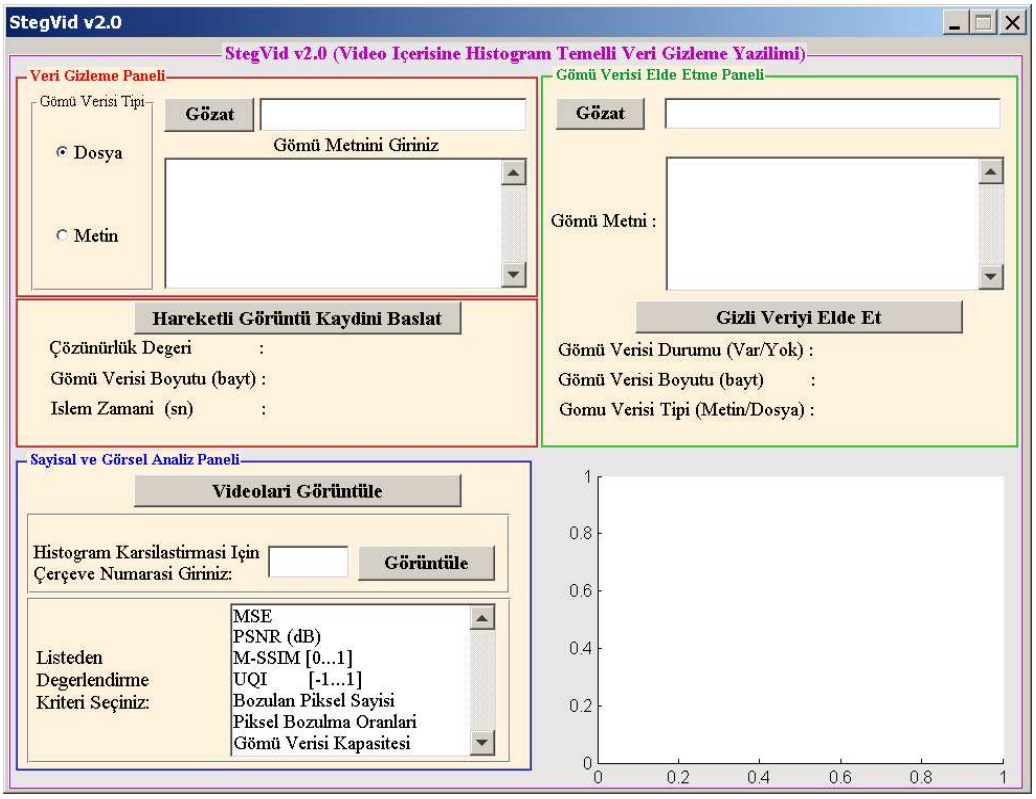


Şekil 4.23: StegVid v1.0'a ait ayrık histogram görüntüleme örneği.



Şekil 4.24: StegVid v1.0'a ait sayısal analiz penceresi.

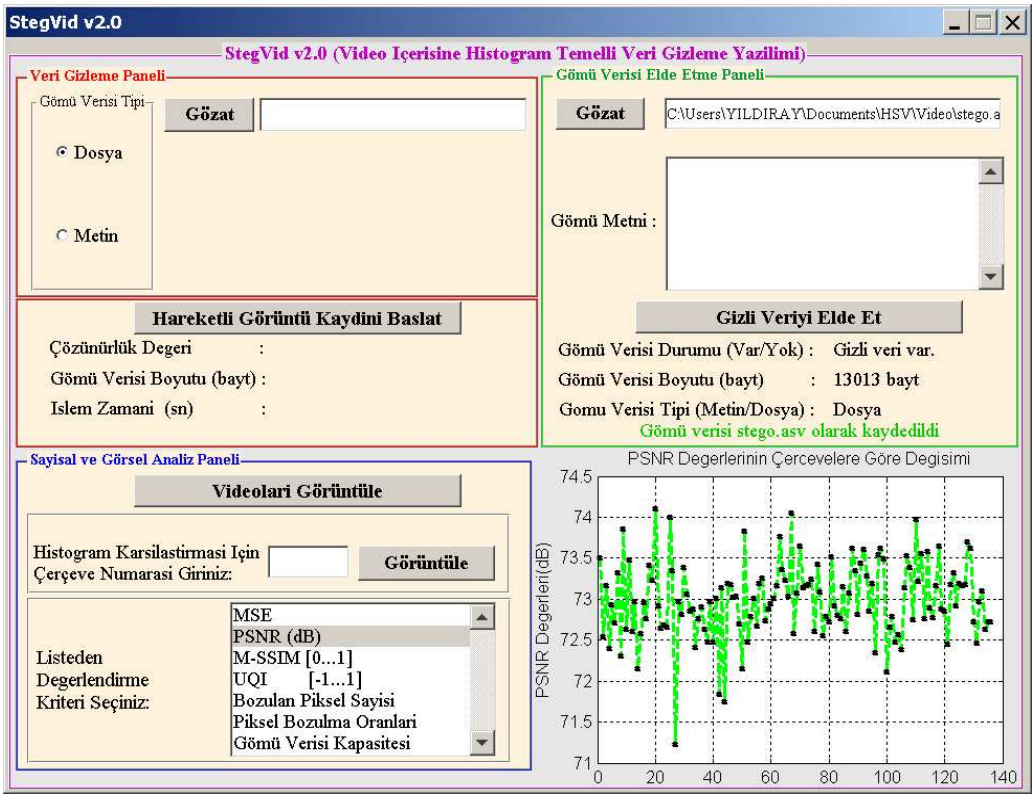
StegVid v2.0 olarak adlandırılan ikinci yazılım ise web kamera yardımı ile gerçek zamanlı alınan sıralı sayısal imgelere HSV yöntemini uygulayarak veri gizleme işlemini gerçekleştirmektedir (Şekil 4.25).



Şekil 4.25: Gerçek zamanlı hareketli görüntü kayıtlarına veri gizleme işlemi yapan StegVid v2.0 arayüzü.

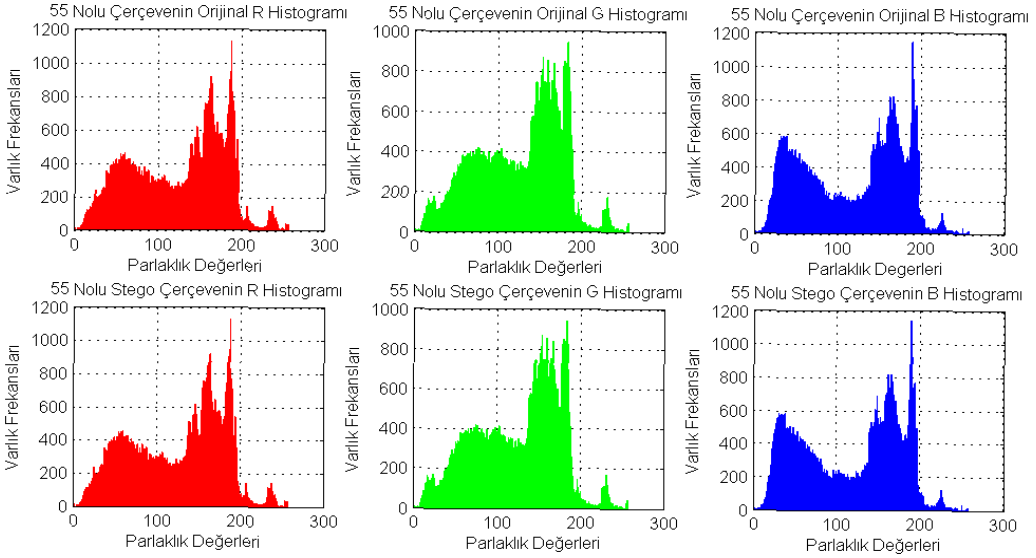
StegVid v2.0 veri gizleme ve gömülü gizli veriyi elde etme işlemlerinin her ikisini de yapabilme kabiliyetine sahip olduğu gibi, hareketli görüntü kayıtlarının görsel (Şekil 4.26) ve sayısal analizlerinin yapılmasını sağlayan özelliklere de sahiptir (Şekil 4.27).

Şekil 4.26: Orijinal ve Stego videoların aynı anda oynatılmasını sağlayan arayüz görünümü.



Şekil 4.27: StegVid 2.0'a ait örnek bir sayısal analiz görünümü.

HSV yönteminin geliştirilmesinde çıkış noktası olan tarak etkisine ilişkin durumun incelenmesini sağlayan histogram analiz penceresi StegVid v1.0'da olduğu gibi StegVid v2.0'da da bulunmaktadır (Şekil 4.28).



Şekil 4.28: StegVid v2.0 video çerçevelerinin histogramlarını görüntüleme penceresi.

4.9. Sonuç

Literatürde veri gizleme amacı temelinde geliştirilen birçok yöntem sunulmuştur. Bu yöntemlerin özünde verilerin mutlak şekilde üçüncü kişilerden gizlenmesi esas alınmaktadır. Bu gizliliğin sağlanması temel olarak taşıyıcıda (örtü verisi) oluşan bozulmaya (gürültü) ve istatistiksel olarak yapılan incelemelerde ortaya çıkan fark edilebilirliğe bağlıdır. Bu temel noktalardan hareketle HSV veri gizleme yöntemi ve uygulama yazılımı StegVid geliştirilmiştir. HSV taşıyıcıda oldukça küçük ve fark edilemez değişimler oluşturarak veri gizlemenin asıl amacına hizmet etmektedir ve bu yönüyle eşleniklerine kıyasla daha öne çıkmaktadır. Takip eden bölümde HSV'nin bu özelliklerini doğrulayan sayısal analizler ve görsel sonuçlar sunulmakta ve detaylı bir şekilde değerlendirilmektedir. StegVid uygulama yazılımı HSV'nin gerçeklenmesini ve farklı başarım ölçütleri açısından değerlendirme yapılmasını sağlamaktadır. Geliştirilen bu yazılım farklı uygulamalardan elde edilen imge (görüntü) ve imgeler dizisinin (video) de değerlendirilmesini sağlamakta ve bu sayede kullanım alanı genişletilmektedir.

5. ÖRNEK StegVid UYGULAMALARI VE BAŞARIM DEĞERLENDİRMESİ

5.1. Giriş

Literatürde veri gizleme bilimi temelinde yapılan çalışmaların büyük çoğunluğunda İGS'ye odaklanan Görsel Karşılaştırma ile Ortalama Karesel Hata (Mean Square Error (MSE)) ve Tepe Sinyal Gürültü Oranı (PSNR) sayısal ölçütleri ön plana çıkmaktadır. Uygulama yazılımı StegVid bu ölçütlere ek olarak literatürde kendisine yer bulmuş, piksel bozulma oranı, histogram analizi, Ortalama Yapısal Benzerlik (Mean Structural Similarity (M–SSIM)) ve Evrensel İmge Kalite İndeksi (Universal Image Quality Index (UQI)) ölçütlerine göre analiz yapılmasını sağlamaktadır. Uygulama yazılımında bulunmayan ancak tez çalışması kapsamında kullanılan farklı ölçütler de mevcut olup, bu ölçütlere ilişkin elde edilen deneysel sonuçlar takip eden alt bölümlerde sunulmaktadır.

5.2. İmge ve İmge Histogramı Üzerinde Görsel Analiz

Sayısal bir imge ve bu imge içerisine veri gizleme söz konusu olduğunda, orijinal görüntüden uzaklaşılması ve bir takım bozulmaların meydana gelmesi kaçınılmaz bir sonuçtur. Önemli olan bu bozulmaların fark edilememesidir. Bozulmaların tespitine dönük ilk çalışma İGS ile yapılan karşılaştırmalara dayanır. Bu karşılaştırmalar genellikle sayısal resmin yaklaştırılması ile ve eğer mevcut ise resmin orijinali ile kıyaslama yapılır. Bu noktada gömü verilerinin oluşturduğu bozulmaların fark edilmemesi (perceptual invisibility) büyük önem taşır. İnceleme sonucunda olağan dışı bir durumun varlığına ilişkin karar verilir.

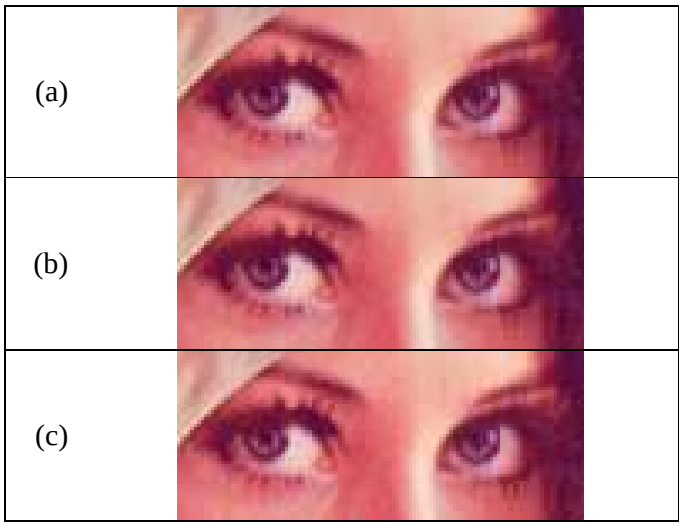
Literatürde veri gizleme çalışmalarında sıklıkla kullanılan Lena, Baboon ve Peppers imgeleri ile bu imgelere StegVid ile veri gizlenmesi sonucunda oluşan stego imgeler Şekil 5.1'de verilmektedir.

(a) (b) (c)

(d) Lena (e) Baboon (f) Peppers

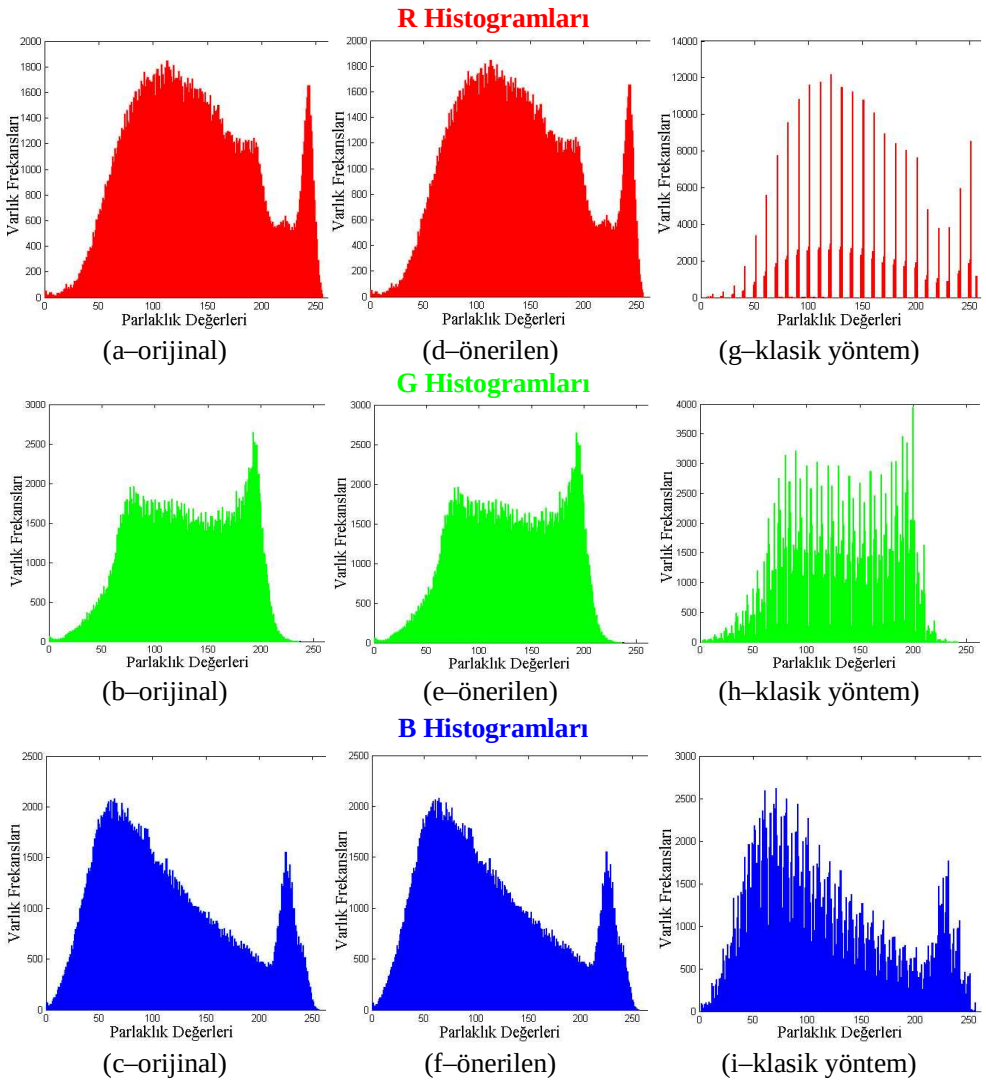
Şekil 5.1: HSV'nin uygulandığı referans resimlerin orijinal (a–b–c) ve veri gizlenmiş görünümleri (d–e–f).

Geliştirilen HSV yöntemi bu karşılaştırma ölçütü açısından çok olumlu sonuçlar vermektedir. Resimlerin orijinalleri mevcut olsa dahi aradaki fark sezilememektedir. Bununla birlikte detaylı inceleme için yakınlaştırma (zoom) işlemi yapıldığında dahi bu durum değişmemektedir (Şekil 5.2).



Şekil 5.2: "Lena" imgesinin (a), HSV (b) ve RGB ağırlık tabanlı kodlama tekniği (c) ile veri gizlendikten sonraki görünümleri.

Şekil 5.2'de Lena imgesi kullanılarak RGB ağırlık tabanlı kodlama tekniği (Akar ve Varol, 2004, Akar, 2005) ve HSV yönteminin görsel analizi yapılmaktadır. Hiç şüphe yok ki gömü verisi içeren örtülü dosyalarda oluşan bozulmalar kodlama tekniklerinin başarısı ile doğrudan ilişkili olduğu kadar, gömülen gizli verinin boyutu ile de ilişkilidir. Bu sebeple veri gizleme uygulamalarında gömü verisi kapasitesi ile imgede oluşan bozulma arasındaki hassas denge en uygun seviyede tutulmalıdır. Yapılan tez çalışmasında doğal görüntü histogramlarının çok düzenli bir yapıda olduğu, sistematik bir bozulma gerçekleştirildiğinde ise histogramlarda tarak etkisinin oluştuğu tespit edilmiştir (Şekil 5.3).



Şekil 5.3: Baboon imgesine ait sırasıyla R, G ve B histogramlarının orijinal (a–b–c), HSV (d–e–f) ve klasik bir yöntem uygulandıktan sonraki (g–h–i) görünümleri.

Şekil 5.3 Baboon imgesinin R, G ve B kanallarına ait histogramlarının orijinal, HSV ve klasik bir yöntemin (Akar ve Varol, 2004) uygulanması sonucundaki ilk ve son durumları hakkında bilgi vermektedir. HSV diğer veri gizleme yöntemlerinin tersine, histogramları gözle algılanabilecek seviyede bozmadığından, gizli veri içeren imge üçüncü kişilerce incelendiğinde şüphe uyandırmamaktadır. Bu sayede muhtemel steganaliz ataklarında gömü verisinin güvenliği üst seviyeye çıkarılmaktadır.

5.3. Piksel Bozulma Oranı

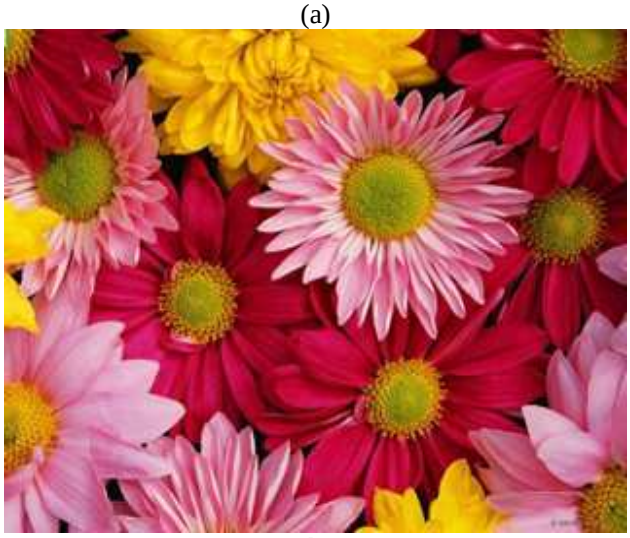
Veri gizleme yöntemlerinin tümü, taşıyıcıda belli oranlarda gürültü oluştururlar ve insanların algılama sistemlerinin hassasiyetindeki zafiyetlerden faydalanırlar. Oluşturulan gürültünün yoğunluğu sezilebilirlik için oldukça önemli bir parametredir. İmgede oluşan gürültü ölçütlerinden biri de piksellerde meydana gelen bozulma oranıdır. Şekil 5.4(a)'da orijinal imge ile (b)'de HSV yöntemiyle kodlanmış imge görülmektedir. Tablo 5.1, HSV yöntemiyle kodlanan imgenin bozulma oranına ait olumlu başarımı açıkça ortaya koymaktadır. HSV yönteminin imge histogramları üzerinde işlem yaptığı düşünüldüğünde, imgenin çözünürlük değeri arttıkça belirtilen oranların daha da azalacağı aşikârdır.

Tablo 5.1: HSV yöntemi ile kodlanan imgenin (Şekil 5.4–b) piksel bozulma oranı başarım tablosu.

Çözünürlük	320×256		
Toplam piksel değeri sayısı	320×256×3= 245760		
Bozulan piksel sayıları	R	G	B
	82	88	57
Bozulma oranı (%)	0,092367		

Bir imge içerisine veri gizlerken değişime uğrayan piksellerin sayısı kadar, ilgili piksellerin değişime uğrama oranının da çok önemli olduğu göz ardı edilmemelidir. Şekil 5.4(c)'de verilen imgedeki bozulan piksel sayıları (b)'de verilen ile aynı olmasına rağmen değişim gözle algılanabilmektedir. Bu sonuçtan hareketle HSV bu yönü ile de çarpıcı sonuçlar vermektedir.

(a)



(b)

(c)

Şekil 5.4: Orijinal (a), HSV ile kodlanmış (b) ve aynı piksel bozulma oranına sahip (c) imgeler.

5.4. Ortalama Karesel Hata (MSE) ve Tepe Sinyal Gürültü Oranı (PSNR)

Literatürde yapılan çalışmaların deneysel sonuçlarının değerlendirilmesi aşamasında, örtülü verinin istatistiksel kalitesini ölçmek için Tepe Sinyal Gürültü Oranı (PSNR) ölçütü sıklıkla kullanılan bir ölçüttür. PSNR, orijinal görüntü ile gömü verisi taşıyan görüntü arasındaki benzerlik kalitesini hesaplar. PSNR, hesaplama sonucunda tek bir değer üretir. Bu değerin yüksek olması kalitenin de yüksek olduğu anlamına gelir.

İki sayısal imge arasındaki PSNR değerini hesaplamak için öncelikle Ortalama Karesel Hata (MSE) değeri hesaplanmalıdır (Jonathan ve diğ., 1999; Sencar ve diğ., 2004; Chang ve diğ., 2008). MSE değerinin hesaplanması için denklem 5.1 veya denklem 5.2 kullanılabilir. MSE değerinin hesaplanmasının ardından denklem 5.3'e göre PSNR değeri hesaplanır (Rabbani ve Jones, 1991; Netravali ve Haskell, 1995).

$$\mathrm{MSE} = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left\| O(i,j) - S(i,j) \right\|^2 \qquad \text{veya} \tag{5.1}$$

$$\mathrm{MSE} = \frac{\sum_{m,n} [O(i,j) - S(i,j)]^2}{m \times n} \tag{5.2}$$

Burada O ve S birbirleriyle kıyaslanan görüntüler olmak üzere; O orijinal imgeyi, S ise elde edilmiş stego imgeyi ifade eder. İmgenin boyutları ise (m×n)'dir. Denklem 5.3'deki MAX değeri imgeye ait bir pikselin almış olduğu en büyük parlaklık değeridir ve genellikle 255 ile ifade edilir.

$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}} \right) \tag{5.3}$$

Yapılan çalışmaların başarımı hakkındaki en iyi fikri, benzer çalışmalardan elde edilen sonuçlarla yapılan karşılaştırmalar verir. Tablo 5.2 gerçekleştirilen çalışmanın 512×512×3 boyutlarına sahip imgeler kullanılarak literatürdeki eşleniği ile PSNR değerleri açısından karşılaştırılmasını sağlayan değerler sunmaktadır.

Tablo 5.2: HSV sonuçlarının literatürdeki benzer bir çalışma ile karşılaştırılması.

	Chrysochos ve diğ. (2007)		**HSV**	
	PSNR Değeri (dB)	**Gömü Verisi (bit)**	**PSNR Değeri (dB)**	**Gömü Verisi (bit)**
Lena	54,12	360	62,75	665
Baboon	53,10	300	59,25	747
Peppers	55,18	300	56,01	700

HSV'nin başarımının daha net şekilde ortaya konulması açısından ilgili test imgelerine aynı miktarda gömü verisinin gizlenmesi sonucunda elde edilen PSNR başarım değerleri Tablo 5.3'te görülmektedir. İlgili değerler dikkate alındığında HSV'nin eşleniğine büyük bir üstünlük sağladığı söylenebilir.

Tablo 5.3: Gömü verisi miktarının aynı olması durumunda oluşan PSNR başarım değerleri.

	Gömü Verisi (bit)	**Chrysochos ve diğ. (2007)**	**HSV**
		PSNR Değeri (dB)	**PSNR Değeri (dB)**
Lena	360	54,12	72,59
Baboon	300	53,10	84,81
Peppers	300	55,18	80,84

Tablo 5.4 ise PSNR değerinin düşürülmesi sonucunu doğuran ancak gömü verisi kapasitesini arttıran bir bakış açısı ile imgenin 32 ayrı parçaya ayrıldıktan sonra verinin gizlenmesi temeline dayalı sonuçları göstermektedir. PSNR değerleri açısından HSV yüksek veri gizleme kapasitesiyle ön plana çıkmaktadır. Ancak veri gizleme algoritmalarının uygulanması sonucunda elde edilecek olan başarım sonuçlarının örtü verisi ve gömü verisi arasındaki benzerliğe bağlı olarak değişkenlik göstereceği unutulmamalıdır.

Tablo 5.4: HSV ile literatürdeki bazı yöntemlerin başarımlarının karşılaştırılması.

Yöntem	**Baboon (512×512×8)**	
	Gömü Verisi (Bit)	**PSNR (dB)**
Honsinger ve diğ. (2001)	<1.024	Belirtilmemiş
Macq and Deweyand (1999)	<2.048	Belirtilmemiş
Fridrich ve diğ. (2001)	1.024	Belirtilmemiş
Tsai (2009)	1.379	23,24
Vleeschouwer ve diğ.(2001)	1.024	29,00
Çelik ve diğ. (2002)	15.176	38,00
Goljan ve diğ. (2001)	2.905	39,00
Hwang ve diğ. (2006)	5.168	48,20
Ni ve diğ. (2006)	5.421	48,20
Kuo ve diğ. (2008)	5.423	48,20
Fallahpour ve Sedaaghi (2007)	5.892	48,35
HSV	6.084	48,37

Tablolardan da görüleceği üzere HSV, PSNR açısından eşleniklerine oranla daha yüksek başarım göstermektedir. Çelik ve diğ. (2002) önerdiği yöntem HSV'ye oranla daha yüksek gömü verisi miktarına sahiptir. Ancak PSNR değeri HSV'ye kıyasla kabul edilebilir seviyede değildir. PSNR değerinin düşük olması önceki bölümde belirtilen görsel karşılaştırmalar açısından olumsuzluk bir sonuç olarak nitelendirilmektedir. Aslında PSNR değeri, İGS ile birebir uyuşan bir sonuç vermemektedir. Çünkü insanların renkleri ve tonları algılama davranışı tamamen birbirinden farklıdır. Bu durum göz önüne alınarak takip eden alt bölümlerde literatürde kendine yer bulmuş farklı yaklaşımlarla HSV'nin sayısal başarım değerlendirmeleri yapılmaktadır.

5.5. Algısal Görünmezlik

Daha önceki bölümlerde de belirtildiği gibi PSNR değeri, İGS ile birebir uyuşan sonuçlar vermemektedir. Çünkü insanların renkleri ve tonları algılama davranışı

tamamen birbirinden farklıdır. Bu sebeple İGS ile daha uyumlu sonuçlar veren ve algısal görünmezlik ölçütleri açısından daha güvenilir olan UQI ve M–SSIM sayısal ölçütleri açısından da HSV sonuçları aşağıda değerlendirilmektedir.

5.5.1. Evrensel kalite indeksi (UQI)

Wang ve Bovik'in 2002 yılında yaptıkları çalışmada ortaya koydukları Evrensel İmge Kalite İndeksi (Universal Image Quality Index: UQI) İGS algılama karakteristiği ile imgelerde oluşan bozulma arasındaki ilişkiye oldukça iyi bir yaklaşım getirmektedir (Şekil 5.5).

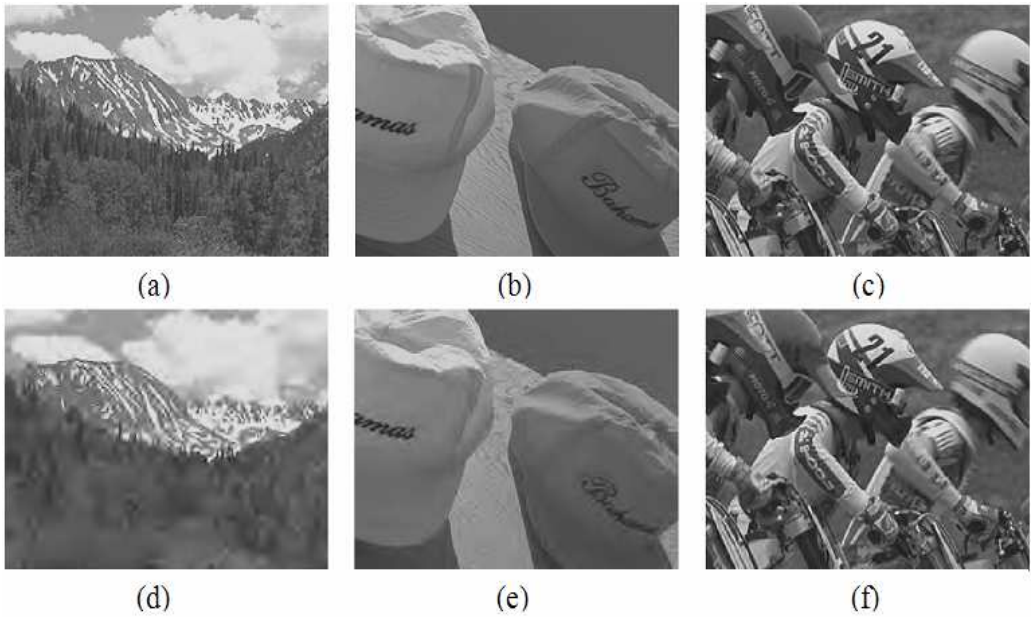
(a) (b) (c) (d)

Şekil 5.5: 512×512 boyutunda orijinal (a), tuz–biber (b) (MSE=225; Q=0,6494), Gauss (c) (MSE=225; Q=0,3891) ve benek (speckle) (d) (MSE=225; Q=0,4408) gürültüsü eklenmiş "Lena" imgesi.

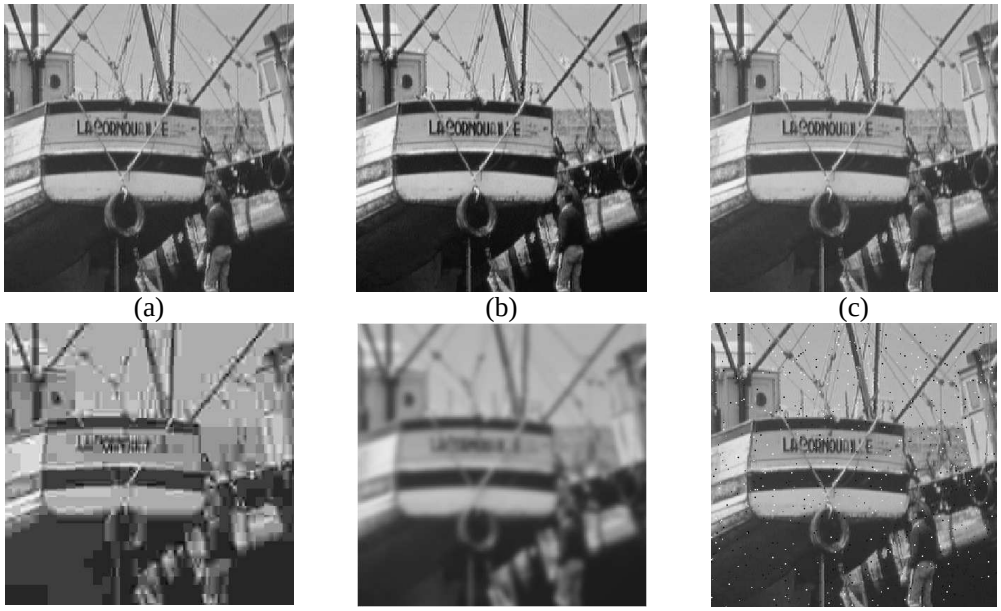
Bu görsel kalite ölçütü [–1…1] aralığında değer alabilen bir kalite (Q) değeri üretir. Kalite yükseldikçe Q değeri 1'e yakınsar. Şekil 5.5'te görüleceği üzere aynı MSE değerlerine sahip olan resimlerin bu ölçüt ile farklı Q değerlerine sahip oldukları ortaya konulmaktadır (Wang ve Bovik, 2002).

5.5.2. Ortalama yapısal benzerlik (M–SSIM)

Benzer şekilde farklı bir istatistiksel yöntemlerle geliştirilen bu yaklaşım 2004 yılında Wang ve arkadaşları tarafından Ortalama Yapısal Benzerlik (Mean Structural Similarity: M–SSIM) adıyla ortaya konulmuştur. Bu yaklaşımda ise [0…1] değer aralığında bir MSSIM değeri üretilir (Şekil 5.6 ve 5.7). Bu kalite ölçütünün geliştirilmesindeki temel motivasyon, MSE ve PSNR değerlerinin İGS açısından objektif sonuçlar vermemesidir (Wang ve diğ., 2004).



Şekil 5.6: Orijinal "Stream" (a), "Caps" (b) ve "Bikes" (c) imgeleri ile PSNR=23,46 dB, MSSIM=0,7339 (d), PSNR=34,56 dB, MSSIM=0,9409 (e), PSNR=33,47 dB, MSSIM=0,9747 (f) değerlerine sahip son görünümleri.



Şekil 5.7: Orijinal “Boat” imgesi (a) ve MSE değerleri 210 olan, karşıtlık yayma işlemi yapılmış (MSSIM = 0,9168) (b), Mean–shift işlemine tabi tutulmuş (MSSIM=0,9900) (c), JPEG yöntemi ile sıkıştırılmış (MSSIM=0,6949) (d), Bulanıklaştırılmış (MSSIM = 0,7052) (e) ve Tuz–biber gürültüsü eklenmiş (MSSIM=0,7748) (f) imgeler.

Şekil 5.7 incelendiğinde, MSE değerleri 210 olan imgeler arasındaki kalite farkı aslında İGS tarafından rahatlıkla algılanabilmektedir. Burada da ortaya çıkan sonuç, MSE ve dolayısı ile PSNR değerinin yetersiz olduğudur. M–SSIM ölçütü açısından da HSV’nin sonuçları diğer kalite ölçütlerinde olduğu gibi eşleniklerine oranla daha iyi sonuçlar vermektedir.

5.5.3. UQI ve M–SSIM açısından HSV sonuçları

Yukarıdaki örneklerden de görüleceği üzere İGS’nin algılayabileceği değişimler olmasına rağmen imgelerin MSE ve PSNR değerleri aynı kalmaktadır. Bu durum MSE’nin dolayısı ile PSNR değerlerinin güvenilirliğinin tam anlamıyla sağlanamadığının bir göstergesidir. Bu sebeple HSV, UQI ve M–SSIM ölçütleri açısından da değerlendirilmiştir. Sayısal imgenin istisnasız tüm en düşük değerlikli bitlerinin (LSB) değişmesi durumunda dahi 512×512 piksel boyutlarındaki “Lena”, “Baboon” ve “Peppers” test imgelerinde, UQI için kalite değeri 0,9999 iken M–SSIM için ise 0,9955 değerini üretmektedir. Bu noktada HSV yönteminin uygulandığı aynı test imgeleri ile yapılan çalışmada UQI için 0,999999 değeri, M–

SSIM için 0,999996 değeri elde edilmiştir. Bu sonuçlar, geliştirilen HSV yönteminin algısal görünmezlik (perceptual invisibility) ölçütleri olan UQI ve M–SSIM açısından da çok iyi başarım gösterdiğini ortaya koymaktadır.

5.6. Çözünürlük Değerleri İle Başarım Sonuçları Arasındaki İlişki

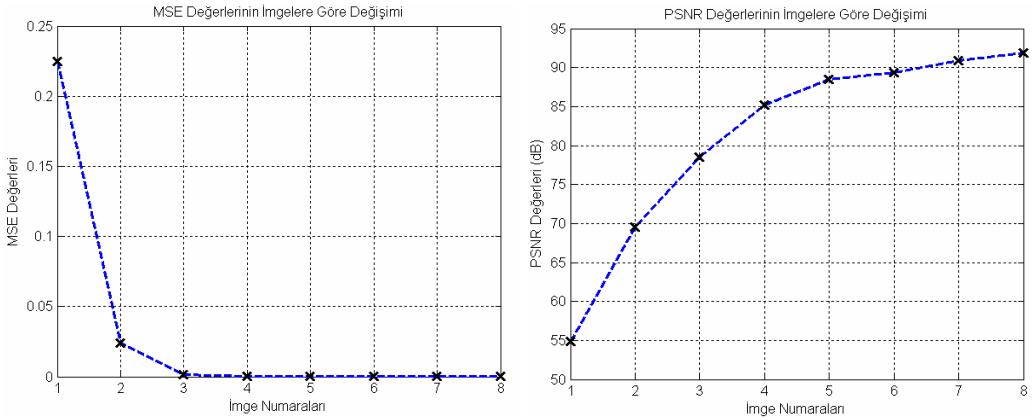
İmge histogramları çözünürlük değerleri ile ilgilenmeden piksellerin renk dağılımlarının bir şema haline getirilmesini sağlarlar. Çözünürlük değerinin artması genellikle histogramlardaki dikey ekseni ifade eden varlık frekanslarının artmasına sebep olurken, bu durum HSV için gömü verisi kapasitesini arttırıcı etki yapmamaktadır (imgeler küçük parçalara ayrılmadığı sürece). Dolayısı ile imgenin çözünürlük değerinin arttırılması halinde, tez çalışması kapsamında geliştirilen HSV'ye ait başarımların da olumlu yönde gelişeceği söylenebilir. Çünkü aynı gömü verisi daha geniş bir örtü verisi içerisine gizlenmiş olacaktır. Bu kapsamda Şekil 5.8'de verilen "SAY" imgesi 8 farklı çözünürlük değerinde HSV yöntemi kullanılarak veri gizleme işlemine tabi tutulmuştur. 74 baytlık aynı gömü verisini taşıyan imgelere ait başarım değerleri Tablo 5.5'te detaylı şekilde verilmektedir.

Şekil 5.8: Farklı çözünürlüklerde HSV ile kodlamak için kullanılan orijinal "SAY" imgesi.

Tablo 5.5: SAY imgesine ait farklı çözünürlük değerlerinde HSV başarım sonuçları.

İmge No	Başarım Ölçütü / Çözünürlük	MSE	PSNR (dB)	M–SSIM	UQI	Bozulan Piksel Sayıları	Piksel Bozulma Oranı (%)
1	256×256	0,2249860	54,8656	0,999955	0,999881	212	0,107830
2	512×512	0,0243047	69,5297	0,999976	0,999960	216	0,027466
3	768×768	0,0016242	78,5259	0,999999	0,999996	228	0,012885
4	1024×1024	0,0002533	85,1899	1	0,999998	224	0,007120
5	1280×1280	0,0001129	88,4674	1	0,999998	225	0,004577
6	1536×1536	0,0000873	89,3200	1	0,999998	223	0,003150
7	1792×1792	0,0000623	90,8847	1	0,999998	206	0,002138
8	2048×2048	0,0000526	91,9096	1	0,999999	203	0,001613

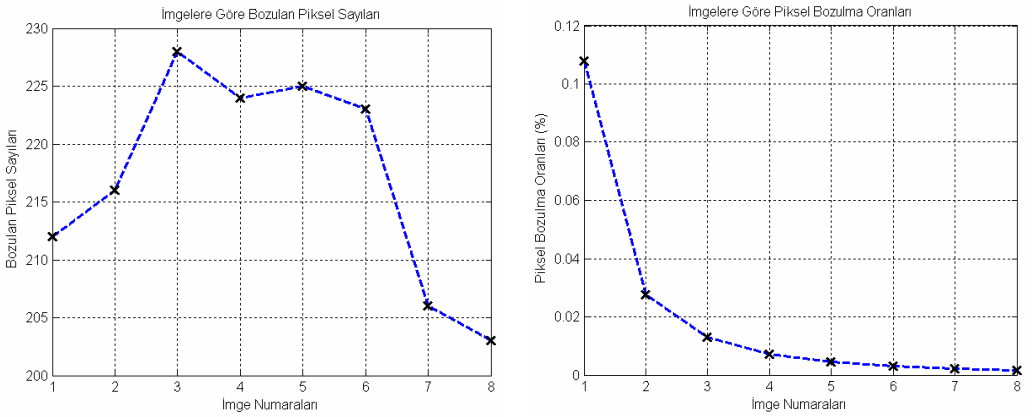
Şekil 5.9'daki MSE ve PSNR başarım grafiklerinden de görüleceği üzere, çözünürlük değerinin arttırılması her iki başarım ölçütü açısından da olumlu sonuçlar alınmasını sağlamaktadır. Veri gizleme uygulamalarında MSE değeri düşük seviyelere çekilirken PSNR değerinin arttırılması hedeflenir.



(a) (b)

Şekil 5.9: Farklı çözünürlük değerlerinde HSV yönteminin MSE (a) ve PSNR (b) başarımları.

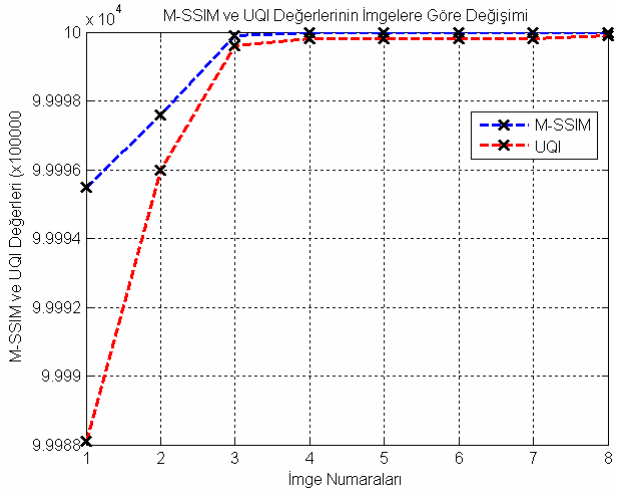
Çözünürlük değerine bakılmaksızın gömü verisi miktarı aynı kaldığı sürece, değişime uğrayan piksel sayıları benzerlik gösterecektir (Şekil 5.10–a). Buna karşılık çözünürlük arttıkça bozulma oranı o ölçüde azalacaktır (Şekil 5.10–b).



(a) (b)

Şekil 5.10: Farklı çözünürlük değerlerinde bozulan piksel sayıları (a) ve oranları (b).

Tez çalışması kapsamında geliştirilen HSV veri gizleme yöntemi, MSE ve PSNR başarım değerlerinde olduğu gibi M–SSIM ve UQI ölçütleri açısından da olumlu sonuçlar vermektedir. Bu sonuçlar içerisinde dikkat edilmesi gereken en önemli nokta, çözünürlük değeri arttıkça ilgili başarımların en yüksek değer olan 1'e ulaşmalarıdır (Şekil 5.11). Bu sonuç insan gözü ile değişimin fark edilmesinin imkânsız olduğuna işaret etmektedir.



Şekil 5.11: Faklı çözünürlük değerlerinde HSV yönteminin M–SSIM ve UQI değerleri.

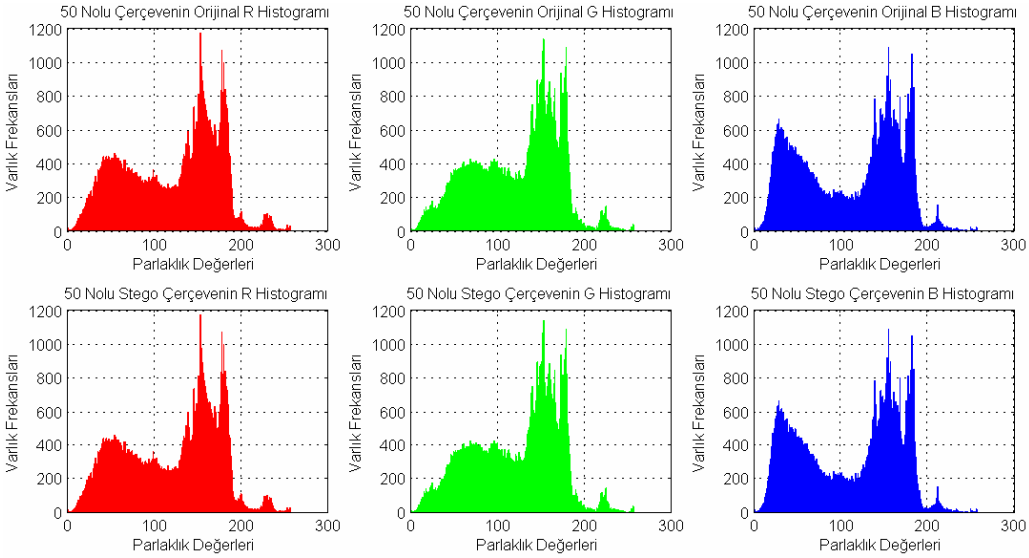
5.7. Gerçek Zamanlı Hareketli Görüntüler İçin Örnek StegVid Sonuçları

Yukarıdaki alt bölümlerde farklı başarım ölçütleri için HSV yönteminin tekil imgelerde ortaya koyduğu sonuçlar verilmektedir. Bu sonuçların hareketli

görüntülerdeki karşılığı ise aşağıda detaylandırılmaktadır. Öncelikle StegVid v2.0 ile gerçek zamanlı hareketli görüntü dosyası elde edilmiş olup (“araba.avi”), bu dosyaya ait bilgiler Tablo 5.6’da verilmektedir. Elde edilen hareketli görüntünün rasgele belirlenmiş bir çerçevesi ve histogramlarının ilk ve son durumları sırasıyla Şekil 5.12 ve Şekil 5.13’te verilmektedir.

(a) (b)

Şekil 5.12: Orijinal çerçeve (a) ve gömü verisi taşıyan stego çerçeve (b).

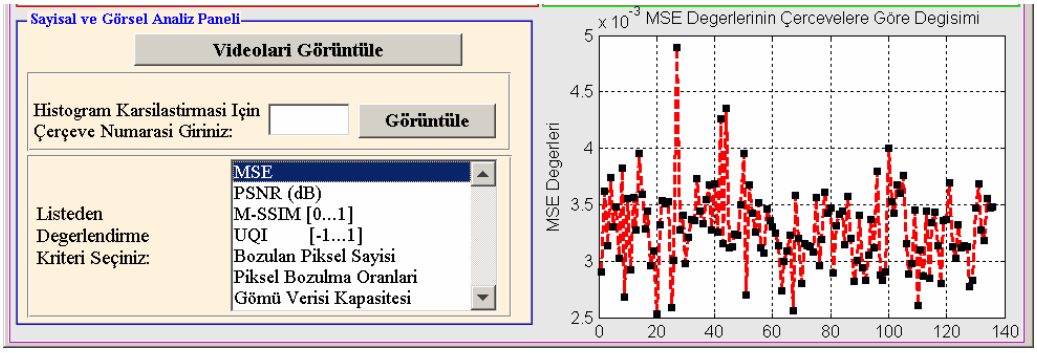


Şekil 5.13: Orijinal ve stego çerçeve histogramları.

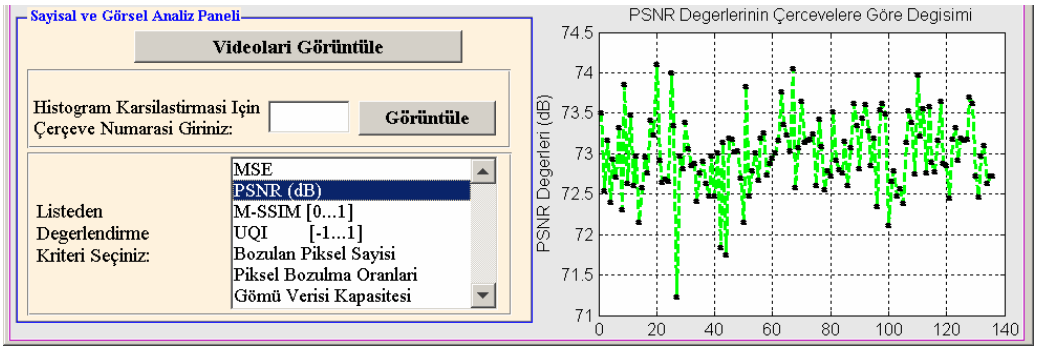
Tablo 5.6: Gerçek zamanlı elde edilen video (“araba.avi”) özellikleri.

Gömü verisi miktarı	13013 bayt
Çerçeve sayısı	136
Çözünürlük değeri	320×240
FPS değeri	30

Daha önceki bölümlerde de ifade edildiği gibi, geliştirilen StegVid yazılımının her iki versiyonu da (v1.0 ve v2.0) farklı başarım ölçütleri açısından imge ve imgeler dizisini analiz edebilmektedir. Yukarıda özellikleri verilen "araba.avi" dosyası ile gömü verisi taşıyan "stego.avi" dosyasının her bir çerçevesinin karşılaştırılması sonucunda elde edilen MSE ve PSNR değerlerini bir grafik üzerinde gösteren StegVid v2.0 görünümleri verilmektedir (Şekil 5.14 ve Şekil 5.15).

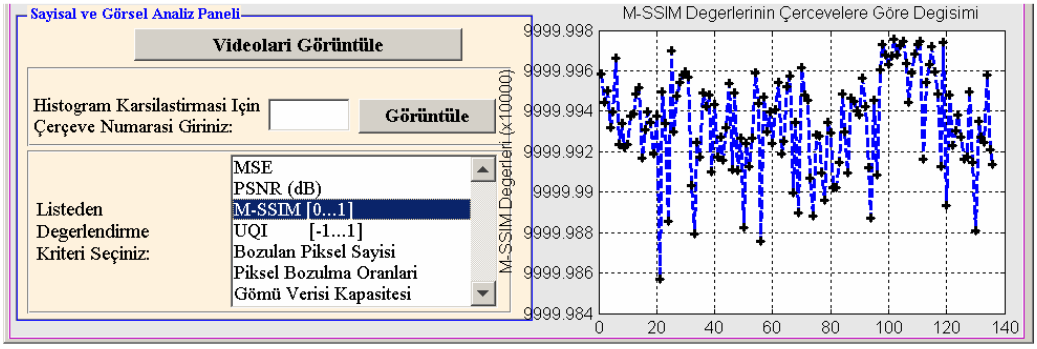


Şekil 5.14: "stego.avi" dosyasına ait MSE değerleri.

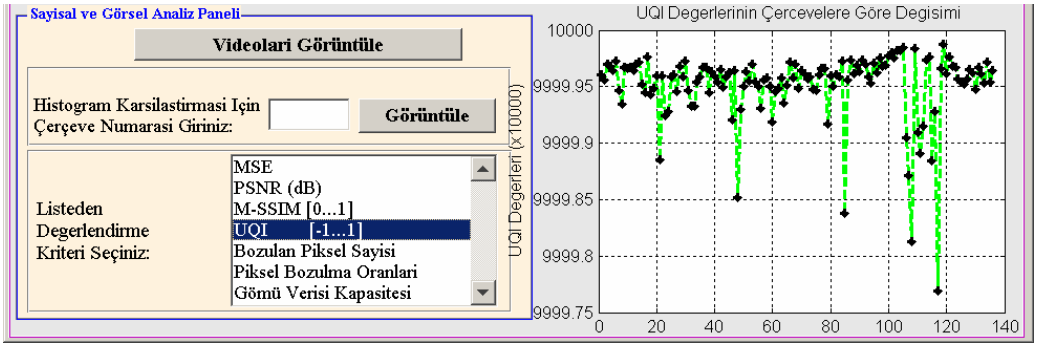


Şekil 5.15: "stego.avi" dosyasına ait PSNR değerleri.

MSE ve PSNR başarım ölçütlerinin İGS ile tam uyumlu olmaması sebebi ile bu metriklere alternatif olarak kullanılan M–SSIM ve UQI değerleri açısından HSV'nin başarımını gösteren StegVid v2.0 görünümleri Şekil 5.16 ve Şekil 5.17'de verilmektedir. Değer aralığı [0…1] arasında olan M–SSIM ve [–1…1] aralığında değer alan UQI başarım ölçütlerinin her ikisinde de HSV'yi kullanarak veri gizleme işlemi yapan StegVid'in en iyi başarım değeri olan 1'e çok yakın sonuçlar ürettiği görülmektedir.

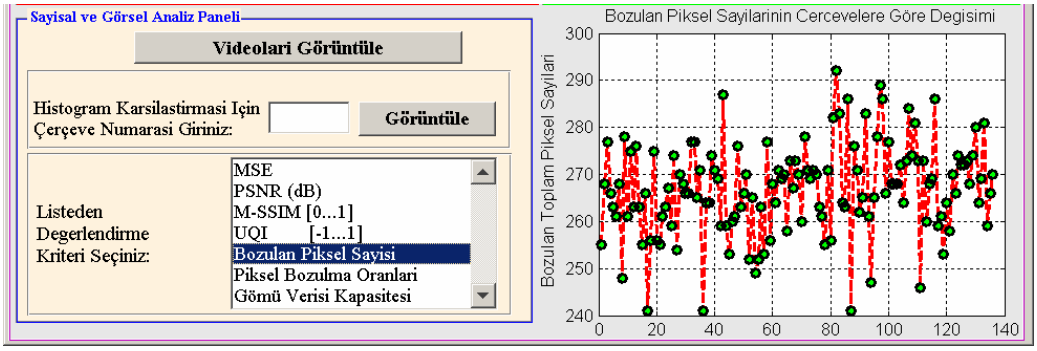


Şekil 5.16: “stego.avi” dosyasına ait M–SSIM değerleri.

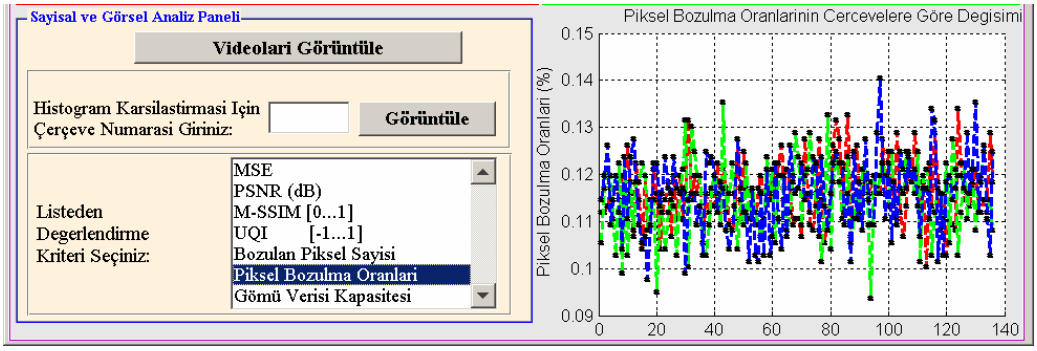


Şekil 5.17: “stego.avi” dosyasına ait UQI değerleri.

Her bir çerçeveye veri gizlendikten sonra oluşan yeni çerçevede bozulmaya uğrayan piksel sayılarını gösteren grafik Şekil 5.18’de verilmektedir. Her bir çerçeveye ait R, G ve B kanallarında oluşan bozulma oranları ise Şekil 5.19’da gösterilmiş olup, her oran kanalların renkleri ile gösterilen çizgiler ile ifade edilmektedir.

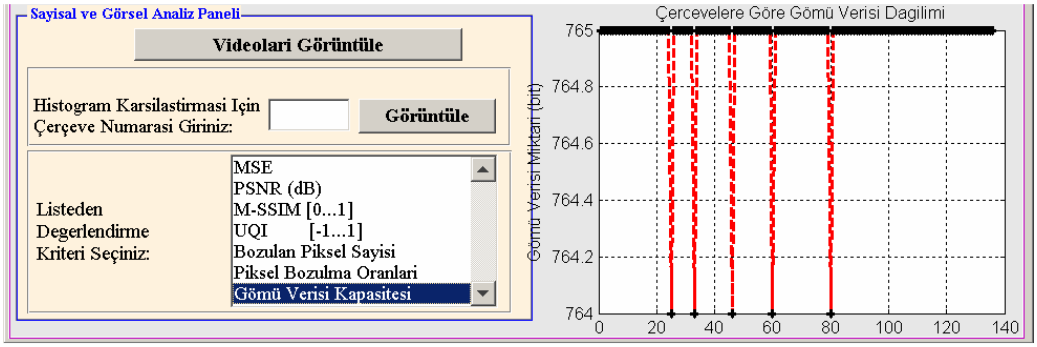


Şekil 5.18: “stego.avi” dosyasına ait bozulan piksel sayıları.



Şekil 5.19: “stego.avi” piksel bozulma oranları.

İmge histogramlarını kullanarak veri gizleme işleminin yapılmasını öngören HSV’nin her bir çerçevede sakladığı veri miktarı Şekil 5.20’de verilmektedir.



Şekil 5.20: “stego.avi” gömü verisi kapasitesi.

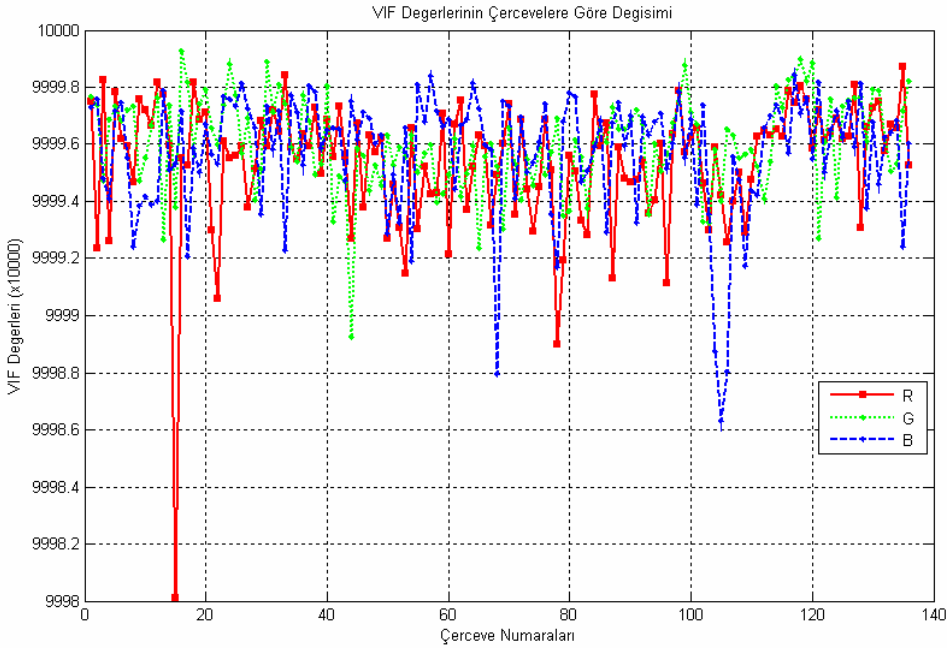
Tablo 5.7’da deneysel çalışmalarda kullanılan ve HSV veri gizleme tekniği ile kodlanmış “stego.avi” dosyasına ait en küçük ve en büyük değerler her bir başarım ölçütü açısından gösterilmektedir.

Tablo 5.7: “stego.avi” dosyasına ait en küçük ve en büyük başarım değerleri.

	En Küçük Değer	**En Büyük Değer**
MSE	0,00253	0,004896
PSNR (dB)	71,23	74,1
M–SSIM	0,9999986	0,9999997
UQI	0,999976	0,999995
Bozulan Piksel Sayısı	241	292
Piksel Bozulma Oranı (%)	0,09375	0,1406
Gömü Verisi Kapasitesi	764	765

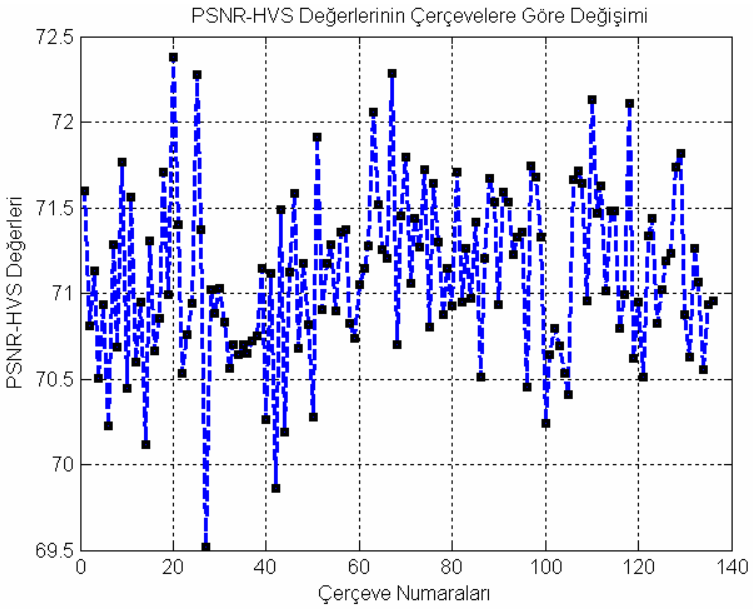
Yukarıda belirtilen başarım ölçütlerinin yanı sıra literatürde tanımlanmış farklı ölçütler de mevcuttur. Bunlardan bazıları Visual Information Fidelity (VIF), Peak Signal to Noise Ratio–Human Visual System (PSNR–HVS), Peak Signal to Noise Ratio–Human Visual System–Modified (PSNR–HVS–M) ve Blind Image Quality Indices (BIQI) şeklinde sıralanabilir. Belirtilen bu ölçütler StegVid yazılımı içerisinde bulunmamaktadır. Ancak elde edilen orijinal ve stego dosyalar StegVid'ten bağımsız olarak bu ölçütler açısından değerlendirmeye tabi tutulmuş olup sonuçlar aşağıda verilmektedir.

MSE değerlerinin İGS ile uyumlu olmadığından hareketle geliştirilen VIF ölçütü [0…1] aralığında bir sonuç üretmektedir ve imgedeki bozulma oranı azaldıkça bu sonuç 1'e yaklaşmaktadır (Sheikh ve Bovik, 2006). "araba.avi" ve "stego.avi" dosyaları kullanılarak elde edilen başarım değerleri Şekil 5.21'de her renk kanalı için ayrı ayrı verilmektedir.



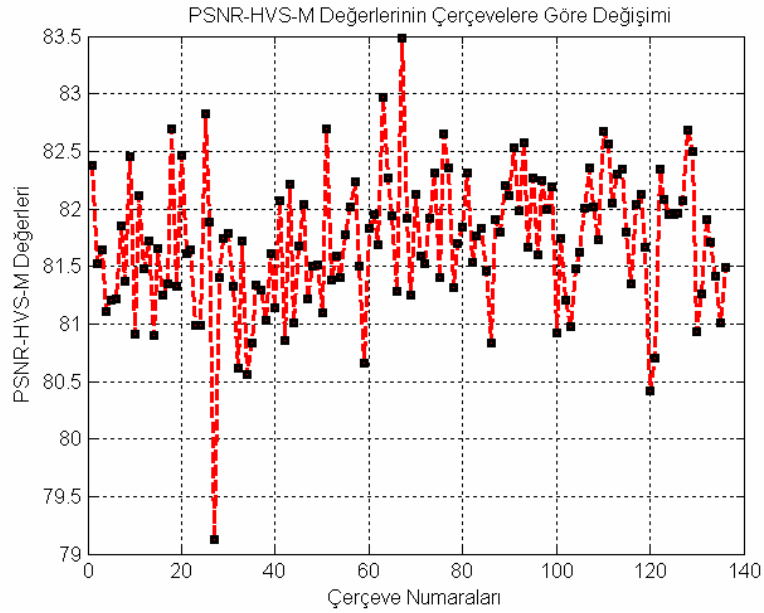
Şekil 5.21: "stego.avi" dosyasına ait VIF değerleri.

PSNR–HVS ölçütü ise DCT katsayı farklarının düzeltme faktörü (correcting factor) adı verilen sabitler ile çarpılması sonucu elde edilen MSE değerlerinin kullanımını sonucu elde edilmektedir (Egiazarian ve diğ., 2006). Şekil 5.22'de PSNR–HVS sonuçları açısından HSV'nin başarımı görülmektedir.



Şekil 5.22: "stego.avi" dosyasına ait PSNR–HVS değerleri.

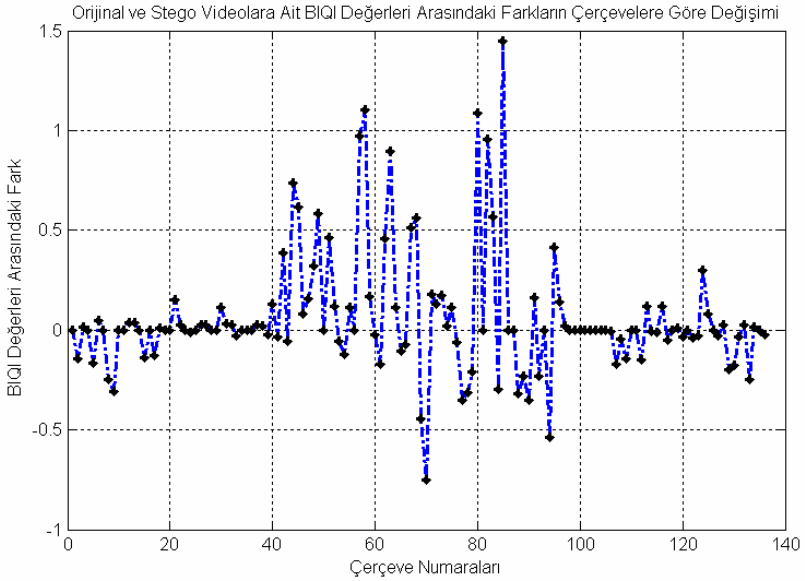
PSNR–HVS–M ölçütünde ise öncelikle orijinal imge ile stego imgenin piksel değerleri arasındaki farkların DCT katsayıları karşıtlık maskeleme işlemine tabi tutularak indirgeme işlemi yapılır. Elde edilen sonuçlar kullanılarak MSE değerleri, ardından PSNR değerleri elde edilir (Ponomarenko ve diğ., 2007). Şekil 5.23'te PSNR–HVS–M ölçütü açısından HSV yönteminin başarımı görülmektedir.



Şekil 5.23: "stego.avi" dosyasına ait PSNR–HVS–M değerleri.

Neredeyse tüm karşılaştırma ölçütleri bozulmaları çeşitli şekillerde ortaya koymak için hem orijinal imgeye hem de stego imgeye ihtiyaç duyarlar. BIQI ölçütü ise bir imgenin kalitesini ölçmek için imgenin sadece kendisine ihtiyaç duymaktadır. Bu ölçüt [0…100] arasında sonuç üretmekte ve elde edilen sayısal değer 0'a yakınlaştıkça imgenin kalitesinin daha iyi olduğu sonucuna varılmaktadır (Moorthy and Bovik, 2010).

Şekil 5.24'te "araba.avi" ve "stego.avi" dosyalarına ait BIQI değerleri arasındaki farkların çerçevelere göre değişimi görülmektedir. BIQI ölçütü sonucu elde edilen değerlerdeki değişim çoğunlukla 0 değerine çok yakın olmakla birlikte, [–0,7…1,4] aralığında değişen küçük farklılıklar oluşmaktadır. Bu sonuç taşıyıcıda oluşan bozulmanın çok düşük seviyelerde olduğuna işaret etmektedir.



Şekil 5.24: "araba.avi" ve "stego.avi" dosyalarına ait BIQI değerleri arasındaki farkların çerçevelere göre değişimi.

Tablo 5.8'de, 136 çerçeveden oluşan ve 320×240 çözünürlüğe sahip "araba.avi" örtü videosu ile HSV yöntemi kullanılarak veri gizlenmesi sonucu oluşan "stego.avi" dosyaları referans alınarak VIF, PSNR–HVS, PSNR–HVS–M ve BIQI ölçütleri açısından elde edilen en küçük ve en büyük başarım değerleri verilmektedir.

Tablo 5.8: HSV yönteminin farklı ölçütler açısından en küçük ve en büyük başarım değerleri.

		En Küçük Değer	En Büyük Değer
VIF		0,9998	1
PSNR–HVS (dB)		69,5207	72,3782
PSNR–HVS–M (dB)		79,1231	83,4826
BIQI	"araba.avi"	20,6060	30,0259
	"stego.avi"	19,9772	30,0259

Yukarıdaki sayısal sonuçlar HSV yönteminin, özellikle fark edilebilirlik ölçütleri açısından literatürdeki eşleniklerine kıyasla daha iyi olduğunu göstermektedir. Bu başarım ölçütlerinden ödün verilerek her bir parlaklık değerinin varlık frekansına 1 bit gömülmesi yerine 2 veya daha fazla bit gömülmesi kapasiteyi arttırıcı bir etken olacaktır. Bununla birlikte kapasite artmasına rağmen tarak etkisi de oluşmayacaktır.

5.8. Sonuç

Veri gizleme yöntemlerinin vazgeçilmez ve en önemli amacı, gömü verisinin üçüncü kişilerin tarafından elde edilememesini ve bozulmamasını sağlamaktır. Yüksek gömü verisi kapasitesi bu şartların ardından sıralanabilecek diğer önemli bir hedeftir. Geliştirilen HSV yönteminin örnek uygulamaları, üçüncü kişilerin hem görsel hem de istatistiksel olarak gömü verisinin varlığını ve gömü verisini tespit edemeyeceklerini ortaya koymaktadır. HSV çıktısı imgede ve özellikle imgeye ait histogram(lar)da yapılan görsel incelemelerde sıra dışı bir durum kesinlikle tespit edilememektedir. Sayısal başarım ölçütü olarak İGS ile uyumlu olmasa da literatürde sıklıkla kullanılan PSNR ölçütü açısından HSV yöntemi, 320×240 çözünürlük değerine sahip bir videoda 74 dB'ye kadar ulaşan bir başarım göstermiştir. İGS ile uyumlu UQI ve M–SSIM ölçütleri açısından da HSV çıktısı imge ve sıralı imgelerde yüksek değer olan 1'e yakın sonuçlar elde edilmektedir. Bununla birlikte son yıllarda literatüre girmiş olan VIF, PSNR–HVS, PSNR–HVS–M başarım ölçütleri açısından da HSV çıktısı stego videolar sırasıyla 1, 72 dB ve 83 dB sonuçlarını vermektedir. Tek bir imgeyi kullanarak bir kalite sonucu üreten BIQI ölçütü kullanılarak elde edilen sonuçlarda da görsel bozulma etkisinin en küçük seviyede tutulduğu tespit

edilmiştir. Şüphesiz bu sonuçlar sayısal imgelerdeki piksellerin bozulma oranının çok düşük seviyelerde olmasından kaynaklanmaktadır. HSV yöntemini temel alarak veri gizleme uygulaması gerçekleştiren ve farklı başarım ölçütleri açısından değerlendirme yapılmasına olanak sağlayan StegVid, farklı uygulamalardan elde edilen sonuç imge ve imge dizilerini de analiz edebilme kabiliyetine sahip olduğundan kullanım alanı genişletilmiş bir yazılım olarak literatüre sunulmaktadır.

6. SONUÇLAR VE ÖNERİLER

Veri gizleme üzerine yapılan çalışmalar, kişisel ve kurumsal bilgi güvenliğinin her geçen gün önem kazandığı günümüzde daha da yaygın bir öneme sahip olmaktadır. Bu tez çalışmasının amacı, bilgi veya verinin korunması için yeni bir yöntem ortaya koymak ve gerçekleştirmektir. Bu amaç doğrultusunda histogram temelli yeni bir veri gizleme yöntemi HSV geliştirilmiş olup, bir uygulama yazılımı (StegVid) ile de gerçeklenmiştir. Geliştirilen yöntem sayesinde yetkisiz/istenmeyen kullanıcılar gizli bilginin ana obje/resim içerisinde olduğundan şüphelenmemektedirler. HSV yöntemi ile sayısal imgeler üzerinde minimum bozulma sağlanarak verinin gizlenmesi, görsel ve istatistiksel olarak fark edilemezliğin sağlanması hedefi gerçeklenmiştir. Önerilen bu yeni yöntem ile bilime ve teknolojiye iki temel katkı sağlanmıştır;

- Klasik birçok yöntemin taşıyıcı imgelere veri gizlemesinin ardından histogramlarda oluşturduğu bozucu etki (tarak etkisi), sunulan tez çalışmasında önerilen veri gizleme yöntemi (HSV) uygulandığında ortaya çıkmamaktadır. Bu sayede histogramın görsel analizinin yapılması sonucunda gömü verisinin varlığından şüphelenilmemektedir.
- Gömü verisinin herhangi bir örneğinin kodlamayı yapan kullanıcı da dâhil hiç kimsede olmamasını sağlamak amacıyla, gerçek zamanlı hareketli görüntüler kullanılarak orijinal veri ile karşılaştırma yapılamaması sağlanarak algılanamazlık ilkesi en üst seviyeye taşınmakta ve geliştirilen uygulama yazılımı (StegVid) ile de bu durum doğrulanmaktadır.

Tez çalışmasının yukarıda ifade edilen ana katkılarının yanı sıra bazı ek özellikleri de bulunmaktadır. Bunlar aşağıda maddeler halinde sıralanmıştır;

- Geliştirilen HSV yöntemi imge histogramlarını kullandığından gömü verisi kapasitesini arttırmak için, imgeler küçük parçalara bölündükten sonra her bir

parçanın histogramına veri gizlenebilmekte yani uygulama esnekliği sağlanabilmektedir.

- İmgedeki piksellerin ya da rasgele bölümlerin yer değiştirmesi sonucunda histogram değişmeyeceğinden gömü verisi kaybolmayacak ya da gömü verisinin dizilişi bozulmayacaktır. Bu da geliştirilen HSV yönteminin, histogramı değiştirmeyen geometrik ataklara karşı dayanıklı olduğunu göstermektedir.
- Özellikle doğal imgelere veri gömülmesi sürecinde ortaya çıkan olumsuz bir durum olan tarak etkisi bu tez çalışmasında detayları ile ortaya konulmuştur. Tez çalışması ile bir imgede gömü verisinin varlığına ilişkin şüphelerin, tarak etkisi ile doğru orantılı olarak artacağı gösterilmektedir.
- Gömü verisinin elde edilmesi sürecinde örtü verisine ihtiyaç duyulmamakta ve örtülü veri kullanılarak gizli veriler elde edilmektedir.
- HSV yöntemi sadece RGB imgelere ve gri tonlu imgelere uygulanabilmektedir.
- StegVid uygulama yazılımı HSV yönteminin gerçeklenmesini ve farklı başarım ölçütleri açısından değerlendirme yapılmasını sağlamaktadır. Geliştirilen bu yazılım farklı uygulamalardan elde edilen imge ve imgeler dizisinin de değerlendirilmesini sağlamakta ve bu sayede kullanım alanı genişletilmektedir.
- Geliştirilen yöntem ile ilgili tüm algoritmalar ve detayları bu çalışma ile sunulduğundan, bir saldırı yönteminin geliştirilmesi kolaylaşmıştır. Tez çalışması ile gerçekleştirilen yöntem bir akademik çalışma ürünüdür ve kodlar açıktır.

Veri gizleme bilimlerinden steganografinin en önemli hedefi, gömü verisinin istenmeyen kişiler tarafından fark edilerek elde edilememesi ve bozulmamasının sağlanmasıdır. Bu hedeften hareketle tez çalışmasının özünü teşkil eden HSV yönteminin eşleniklerine kıyasla daha olumlu sonuçlar verdiği görülmektedir.

6.1. Öneriler

Geliştirilen HSV yönteminin kolay şekilde gerçeklenebilmesi ve değiştirilerek geliştirilmesi mümkündür. Bu noktadan hareketle sunulan bu tez çalışmasından esinlenerek, bir takım veri gizleme çalışmaları gerçekleştirilebilir. Bunlar aşağıdaki şekilde sıralanabilir:

- Gömü dosyası/metni bilgileri için başlık bilgisinde belirlenen alanlar arttırılarak, HSV'nin uygulandığı hareketli görüntü kayıtlarındaki veri gizleme kapasitesinin üst sınırı arttırılabilir (tez çalışmasında bu sınırlar dosya için 16 MB, metin için ise 65536 karakterdir).
- Bir imge içerisinde gizli veri olmadığı halde gömü verisi var bilgisinin oluşma ihtimali çok küçükte olsa (2^{-24}) mevcuttur. Tasarlanan yöntemin esnek yapısı sayesinde, bu olasılık kullanılacak daha uzun başlat örüntüsüyle azaltılabilir.
- Gömü verisi varlığına dair başlık bilgisi ilk çerçeveye yerleştirildiğinden, ilgili çerçeve çok büyük önem taşımaktadır. Bu çerçevenin zarara uğrama ihtimali düşünülerek başlık bilgisi belli aralıklarla farklı çerçevelere yerleştirilebilir.
- Gömü verisi kapasitesini arttırma amacıyla imgeler belirlenecek sayıda parçaya ayrılarak ilgili parçaların histogramlarına HSV uygulanabilir.
- Yapılan çalışmalar sayısal imgelere odaklandığından video içerisinde örtü verisi olarak sadece imgeler kullanılmaktadır. Ancak gömü verisinin bir kısmı imgeler bir kısmı ise videodaki ses bilgilerine gömüldüğünde kapasite arttırılmış olacaktır.
- Geliştirilen uygulamada, gizli veriler sayısal imgeler içerisine şifrelenmeden yerleştirilmektedir. Gömü verisinin bir şifreleme fonksiyonu yardımı ile şifrelenmesi ile güvenlik daha üst seviyelere taşınabilir. Günümüzde geliştirilmiş dosya sıkıştırma programları sıkıştırma sırasında bir şifre üreterek dosyayı koruma altına almaktadır. Bu sebep ile gerçeklenen tez çalışmasında ayrıca bir şifreleme tekniği üzerinde durma gereksinimi duyulmamıştır. Fakat bir şifreleme yönteminin çalışma ile bütünleştirilmesi StegVid'in esnek yapısı sayesinde kolaylıkla sağlanabilir.
- HSV yönteminin uygulanmasını sağlayan ve sunulan tez çalışması kapsamında geliştirilen uygulama yazılımı StegVid, veri gizleme amacıyla kullanılmaktadır. StegVid yazılımı küçük değişikliklerle geniş alan ağlarında gerçek zamanlı gizli haberleşme amacıyla kullanılabilir ve kullanım alanı çok daha geniş alanlara yayılabilir.
- Tez çalışması kapsamında geliştirilen HSV yönteminin daha etkin ve verimli şekilde kullanımı donanımsal bir uygulama (FPGA vb.) ile gerçekleştirilebilir.

KAYNAKLAR

Ahmed, N., Natarajan, T., Rao, K. R., "Discrete cosine transform", ***IEEE Transactions on Computers***, C−23, 90−93, (1974).

Akar, F., "Veri gizleme ve şifreleme tabanlı bilgi güvenliği uygulaması", Doktora Tezi, ***Marmara Üniversitesi***, (2005).

Akar, F., Varol, H. S., "A new RGB weighted encoding technique for efficient information hiding in images", ***Journal of Naval Science and Engineering***, 2, 21−36, July (2004).

Akbal, T., "Ses verilerine sıkıştırılmış ve şifrelenmiş ham verilerin gömülmesi", Yüksek Lisans Tezi, ***Sakarya Üniversitesi***, (2008).

Akbal, T., Yalman, Y., Özcerit, A.T., "Gerçek zamanlı sayısal ses içerisinde sıkıştırılmış ve şifrelenmiş veri transferi", ***III. Ağ ve Bilgi Güvenliği Sempozyumu***, Çankaya Üniversitesi, Ankara, 5–6 Şubat (2010).

Anderson, R.J., "Information hiding: first international workshop", ***Lecture Notes in Computer Science***, Isaac Newton Institute, Springer Verlag, Berlin, Germany, ISBN 3−540−61996−8, 1996.

Bandırmalı, N., "Yeni bir kablosuz algılayıcı ağ veri bağı katmanı güvenlik protokolü tasarımı", Doktora Tezi, ***Kocaeli Üniversitesi***, (2010).

Barni, M., Bartolini, F., "Watermarking systems engineering enabling digital assets security and other applications", ***Marcel Dekker Inc***., New York, (2004).

Barni, M., Bartolini, F., Checcacci, N., "Watermarking of MPEG−4 video objects", ***IEEE Transactions on Multimedia***, 7(1), 23−32, (2005).

Barton, J. M., "Method and apparatus for embedding authentication information within digital data", ***United States Patent:*** 5,646,997, (1997).

Bhatnagar, G., Raman B., "A new robust reference watermarking scheme based on DWT–SVD", ***Computer Standards & Interfaces***, 31(5), 1002–1013, (2009).

Bothun, G., 2010, *The electronic universe an educational outreach server*, University of Oregon, http://zebu.uoregon.edu/~imamura/122/images/ **(Ziyaret Tarihi: 20 Temmuz 2010)**.

Braudaway, G.W., “Protecting Publicly–available images with an invisible image watermark”, ***IEEE International Conference on Image Processing***, 2, 1024–1025, (1997).

Brigham, E. O., “The fast fourier transform”, Englewood Cliffs, ***NJ: Prentice−Hall***, (1974).

Brunton, A., Zhao, J., “Real–time video watermarking on programmable graphics hardware”, ***IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)***, 1312–1315, 1–4 May (2005).

Candan, Ç., “Minimum distortion data hiding for compressed images”, PhD. Thesis, ***Georgia Institute of Technology***, (2004).

Caronni, G., “Assuring ownership rights for digital images”, ***Proceedings of Reliable IT Systems***, VIS–95, (1995).

Cetin, O., Ozcerit, A.T., “A new steganography algorithm based on color histograms for data embedding into raw video streams”, ***Computers & Security***, 28, 670–682, (2009).

Chang, C.C., Lin, C.C., Chen, Y.H., “Reversible data–embedding scheme using differences between original and predicted pixel values”, ***IET Information Security***, 2, 35–46, (2008).

Chrysochos, E., Fotopoulos, V., Skodras, A., Xenos, M., “Reversible image watermarking based on histogram modification”, ***11th Panhellenic Conference on Informatics with International Participation***, Greece, B, 93–104, 18–20 May (2007).

Cox, I.J., Kilian, J., Leighton, F., Shamoon, T., “Secure spread spectrum watermarking for multimedia”, ***IEEE Transactions on Image Processing***, 6(12), 1673–1687, (1997).

Cox, I.J., Miller, M.L., Bloom, J.A., “Watermarking applications and their properties”, ***IEEE International Conference on Information Technology (ICCIT)***, Las Vegas, USA, 1–5, 27–29 March (2000).

Celik, M.U., Sharma, G., Tekalp, A.M., Saber, E., “Reversible data hiding”, ***Proc. of IEEE International Conference of Image Processing***, 2, 157–160, (2002).

Çetin, Ö., “Hareketli görüntü uygulamaları için sırörtme yaklaşımı ile veri gömme algoritması tasarımı”, Doktora Tezi, ***Sakarya Üniversitesi***, (2008).

Dai, Y., Zhang, L., Yang, Y., “A new method of mpeg video watermarking technology”, ***IEEE International Conference on Communication Technology***, 1845–1847, (2003).

Delaigle, J. K., "Protection of intellectual property of images by perceptual watermarking", Doktora Tezi, ***Universitè Catholique de Louvain***, (2000).

Doerr, G., Dugelay, J.L., "Security pitfalls frame–by–frame approaches to video watermarking", ***IEEE Transactions on Signal Processing***, 52(10), 2955–2964, (2004).

Echizen, I., Tanimoto, K., Yamada, T., Dainaka, M., Tezuko, S., Yoshiura, H., "PC–based real–time watermark system with standard video interface", ***IEEE International Conference on Systems, Man and Cybernetics***, Taiwan, 267–271, 8–11 October, (2006).

Egiazarian, K., Astola, J., Ponomarenko, N., Lukin, V., Battisti, F., Carli, M., "New full–reference quality metrics based on HVS", "***CD–ROM Proceedings of the Second International Workshop on Video Processing and Quality Metrics***", Scottsdale, USA, 4 p, (2006).

Erçelebi, E., Subaşı, A., "Robust multi bit and high quality audio watermarking using pseudo–random sequences", ***Computers and Electrical Engineering***, 31, 525–536, (2005).

Fallahpour, M., Sedaaghi, M.H., "High capacity lossless data hiding based on histogram modification", ***IEICE Electronics Express***, 4, 205–210, (2007).

Fridrich, J., Goljan, M., Du, R., "Invertible authentication", ***Proc. of SPIE Security Watermarking Multimedia Contents***, Canada, pp. 197–208, (2001).

Goljan, M., Fridrich, J., Du, R., "Distortion–free date embedding for images", ***Proc. of 4th Information Hiding Workshop***, USA, 27–41, (2001).

Gonzalez, R., Woods, R.E., "Digital image processing", ***Prentice Hall Upper Saddle River***, ISBN 0–201–18075–8, New Jersey, (2002).

Gruhl, D., Bender, W., Lu A., "Echo hiding", ***ISBN 3–540–61996–8***, (1996).

Hartung, F., Kutter, M., "Multimedia watermarking techniques", ***Proceedings of the IEEE***, 87(7), 1079–1107, (1999).

Ho, Y.A., Chan, Y.K., Wu, H.C., Chu, Y.P., "High capacity reversible data hiding in binary images using pattern substitution", ***Computer Standards and Interfaces***, 31(4), 787–794, (2009).

Hongmei, L., Zhefeng, Z., Jiwu, H., Xialing, H., Shi, Y.Q., "A high capacity distortion–free data hiding algorithm for palette image", ***IEEE International Symposium on Circuits and Systems (ISCAS '03)***, 2, 916–919, (2003).

Honsinger, C. W., Jones, P., Rabbani, M., Stoffel, J. C., "Lossless recovery of an original image containing embedded data", ***United States Patent:*** 6,278,791, (2001).

Huang, H.C., Fang, W.C., "Intelligent multimedia data hiding techniques and applications", ***IEEE International Conference on Information Security and Assurance***, 477–482, 24–26 April (2008).

Hwang, J.H., Kim, J.W., Choi, J.U., "A reversible watermarking based on histogram shifting ", ***5th International Workshop on Digital watermarking (IWDW)***, Jeju Island, 348–361, (2006).

Johnson, N.F., Jajodia, S., "Exploring steganography: seeing the unseen", ***IEEE Computer***, (1998).

Jonathan, K.S., Hartung, F., Girod, B., "Digital watermarking of text, image and video documents", ***Computer & Graphics***, 22(6), 687–695, December (1999).

Jung, H.K., Yoo, K.Y., "Data hiding method using image interpolation", ***Computer Standards & Interfaces***, 31(2), 465–470, (2009).

Karlsson, J., Li, H., Eriksson, J., "Real–time video over wireless ad–hoc networks", ***14th International Conference on Communications and Networks (ICCCN'05)***, 596, 17–19 October (2005).

Kim, H.Y., Queiroz, R.L.D., "A public–key authentication watermarking for binary images", ***IEEE International Conference on Image Processing (ICIP)***, Singapore, 3459–3462, 24–27 October (2004).

Kuo, W.C., Jiang, D.J., Huang, Y.C., "A Reversible data hiding scheme based on block division", ***Congress on Image and Signal Processing***, 1, 365–369, 27–30 May (2008).

Lee, C.H., Oh, H.S., Lee, H.K., "Adaptive video watermarking using motion information", ***Proceedings of SPIE***, San Jose, USA, 209–216, 24 January (2000).

Lian, S., Liu, Z., Ren, Z., Wang, H., "Commutative encryption and watermarking in video compression", ***IEEE Transactions on Circuits and Systems for Video Technology***, 17(6), 774−778, (2007).

Liang, H., Ran, W., Nie, X., "A secure and high capacity scheme for binary images", ***Proceedings of the ICWAPR***, 224–229, (2007).

Lin, C.C., Tai, W.L., Chang, C.C., "Multilevel reversible data hiding based on histogram modification of difference images", ***Pattern Recognition***, 41, 3582–3591, (2008).

Liu, H.H., Chang, L.W., "Real–time digital video watermarking for digital rights management via modification of VLCS", ***IEEE Proc. of 11th Int. Conference on Parallel and Distributed Systems (ICPADS'05)***, Fukuoka, 295–299, 22 July (2005).

Longmei, L., Zhefeng, Z., Jiwu, H., Xialing, H., Shi, Y.Q., "A high capacity distortion–free data hiding algorithm for palette images", ***IEEE International Symposium on Circuits Sytems***, 2, 916–919, 25–28 May (2003).

Macq, B. and Deweyand, F., "Trusted headers for medical images", ***DFG VIII–D II Watermarking Workshop***, Germany, (1999).

Malvar, H.S., Florencio, D.A.F., "Improved spread spectrum: A new modulation technique for robust watermarking", ***IEEE Transactions on Signal Processing***, 51(4), 898–905, (2003).

Marvel, L., Retter, C. T., Boncelet, C. G., "A methodology for data hiding using images", ***IEEE Military Communications Conference (MILCOM'98)***, 3, 1044–1047, (1998).

Meka, H., "Encryption, watermarking and steganography in application to biometrics", MSc. Thesis, ***Lena Department of Computers Science and Electrical Engineering***, West Virginia, (2007).

Menezes, A. J., Oorschot, P. C., Vanstone S. A., "Handbook of applied cryptography", ***CRC Press***, (1997).

Moorthy, A. K., Bovik, A. C., "A two–step framework for constructing blind image quality indices", ***IEEE Signal Processing Letters***, 17(5), 513–516, (2010).

Moradi, S., Gazor, S., "Evaluation of robust interframe mpeg video watermarking", ***IEEE Canadian Conference on Electrical and Computer Engineering***, Saskatchewan, Canada, 1923–1926, 1–4 May (2005).

Netravali, A.N., Haskell, B.G., "Digital pictures: representation, compression and standards", ***Plenum Press (2nd Edition),*** New York, NY, (1995).

Ni, Z., Shi, Y.Q., Ansari, N. and Su, W., "Reversible data hiding", ***IEEE Transactions on Circuits and Systems for Video Technology***, 16, 354–362, (2006).

Ni, Z., Shi, Y. Q., Ansari, N., Su, W., Sun, Q., Lin, X., "Robust lossless image data hiding designed for semi fragile image authentication", ***IEEE Transactions on Circuits and Systems for Video Technology***", 18(4), 497–509, (2008).

Papapanagiotou, K., Kelliniz, E., Marias, G.F., Georgiadis, P., "Alternatives for multimedia messaging system steganography", ***IEEE International Conference on Computational Intelligence and Security***, Xian, China, 589–596, December (2005).

Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G., "Information hiding–a survey", ***Proceedings of the IEEE, Special Issue on Protection of Multimedia Content***, 87(7), 1062–1078, (1999).

Pfitzmann, B., "Information hiding terminology", ***Information Hiding Workshop***, LNCS,Springer–Verlag, Cambridge, UK, 1996.

Ponomarenko, N., Silvestri, F., Egiazarian, K., Carli, M., Lukin, V., "On between–coefficient contrast masking of DCT basis functions", ***CD–ROM proceedings of Third International Workshop on Video Processing and Quality Metrics for Consumer Electronics VPQM–07***, 4 p, (2007).

Pratt, W.K., "Digital image processing", ISBN: 978–0–471–76777–0, ***John Wiley & Sons Inc.***, Hoboken, New Jersey, (2007).

Provos, N., Honeyman, P., "Hide and seek: an introduction to steganography", ***IEEE Security & Privacy***, 1(3), 32−44, (2003).

Rabah, K., "Steganography−The art of hiding data", ***Information Technology of Journal***, 3(3), 245−269, (2004).

Rabbani, M., Jones, P.W., "Digital image compression techniques", ***SPIE Optical Engineering Press***, Bellvue, Washington (1991).

Rioul, O., Duhamel, P., "Fast algorithms for wavelet transforms", ***IEEE Transaction on Information Theory***, 38(2), 569−586, (1992).

Santis, M.D., Spagnolo, G.S., "Asymmetric cryptography as subset of digital hologram watermarking", ***14th European Signal Processing Conference (EUSIPCO)***, Florence, Italy, 4−8 September (2006).

Sencar, H.T., Ramkumar, M., Akansu, A.N., "Data hiding fundamentals and Applications", ***Elsevier Academic Press***, New York, (2004).

Schyndel, R., Tirkel, A., Osborne, C., "A digital watermark", ***Proceedings of the IEEE International Conference on Image Processing***, 2, 86–90, (1994).

Schneier, B., "Applied cryptography", ***John Wiley and Sons***, (1996).

Shahreza, M.S., "A new method for real–time steganography", ***IEEE 8th International Conference on Signal Procesing (ICSP)***, 4, 16–20 November (2006).

Shahreza, M.H.S., Shahreza, M.S., "Sending mobile software activation code by sms using steganography", ***IEEE 3rd International Conference on International Information Hiding and Multimedia Signal Processing (IIH–MSP 2007)***, 554–557, (2007).

Sheikh, H. R., Bovik, A. C., "Image information and visual quality", ***IEEE Transactions on Image Processing***, 15, 430–444, (2006).

Tadiparthi, G.R., Sueyoshi, T., "A novel steganographic algorithm using animations as cover", ***Decision Support Systems***, 45(4), 937–948, (2008).

Tanaka, K., Nakamura, Y., Matsui, K., "Embedding a secret information into a dithered multi–level image", ***Proceedings of IEEE Military Communications Conference***, 216–220, (1990).

Taşkın, D., Suçsuz, N., "Sıkıştırılmış ortamda çerçeve tipine dayalı gerçek zamanlı sahne değişimi belirleme", ***IV. Bilgi Teknolojileri Kongresi, Akademik Bilişim***, Pamukkale Üniversitesi, (2006).

Tekalp, A. M., "Digital video processing", ***Prentice Hall***, (1995).

Tektaş, M., Baba, F., Çalışkan, E.M., "Şifreleme algoritmalarının sınıflandırılması ve bir kredi kartı uygulaması", ***3rd International Advanced Technologies Symposium***, Ankara, 18–20 Ağustos (2003).

Tian, J., "Reversible data embedding using a difference expansion", ***IEEE Transaction on Cicuits and Systtems for Video Technology***, 13(8), 890–896, (2003).

Tsai, P., "Histogram–based reversible data hiding for vector quantization–compressed images", ***IET Image Processing***, 3, 100–114, (2009).

Tsai, P., Hu, Y. C., Yeh, Y. L., "Reversible image data hiding scheme using predictive coding and histogram shifting", ***Signal Processing***, 89(6), 1129–1143, (2009).

Verheul, E., Koops, B., Tilborg, H.V., "Public key infrastructure binding cryptography", A Fraud–Detectible Alternative To Key–Escrow Proposals Computer Law & Security Report, ***Elsevier Science***, 13(1), (1997).

Vleeschouwer, C.D., Delaigle, J.F., Macq, B., "Circular interpretation on histogram for reversible watermarking", ***Proc. of IEEE International Multimedia Signal Processing Workshop***, France, 345–350, (2001).

Wang, Z., Bovik, A.C., "A universal image quality index", ***IEEE Signal Processing Letters***, 9, 81–84, (2002).

Wang, Z., Bovik, A.C., Sheikh, H.D., Simoncelli, E.P., "Image quality assessment: from error visibility to structural similarity", ***IEEE Transactions on Image Processing***, 13, 600–612, (2004).

Wang, H., Wang, S., "Cyber warfare: steganography vs. steganalysis", ***Communications of the ACM***, 47(10), 76–82, (2004).

Wolfgang, R.B., Delp, E.J., "A watermark for digital images", ***Proceedings of the IEEE International Conference on Image Processing***, Lausanne, Switzerland, 111, 219–222, (1996).

Wu, M., "Multimedia data hiding", PhD. Thesis, ***Princeton University***, 2001.

Venkatraman, S., Abraham A., Paprzycki, M., "Significance of steganography on data security, ***IEEE Proceedings of the International Conference on Information Technology***, 2, 347–351, (2004).

Yalman, Y., “Sayısal ses içerisinde gizli veri transferinin kablosuz ortamda gerçekleştirilmesi”, Yüksek Lisans Tezi, ***Kocaeli Üniversitesi***, (2007).

Yalman, Y., Ertürk, İ., “Sayısal ses içerisinde gizli metin transferinin kablosuz ortamda gerçekleştirilmesi”, ***Ulusal Teknik Eğitim, Mühendislik ve Eğitim Bilimleri Genç Araştırmacılar Sempozyumu (UMES’07)***, 41–45, 20–22 Haziran (2007).

Yalman, Y., Ertürk, İ., “Sayısal ses içerisinde gizli veri transferinin kablosuz ortamda gerçekleştirilmesi”, ***Gazi Üniversitesi Politeknik Dergisi***, 11(4), 319–327, (2008).

Yalman, Y., Ertürk, İ., “İmge histogramı kullanılarak geometrik ataklara dayanıklı yeni bir veri gizleme tekniği tasarımı ve uygulaması”, ***XI. Akademik Bilişim Konferansları***, Harran Üniversitesi, Şanlıurfa, 537–544, 11–13 Şubat (2009a).

Yalman, Y., Ertürk, İ., “Gerçek zamanlı video kayıtlarına veri gizleme uygulaması”, ***XI. Akademik Bilişim Konferansları***, Harran Üniversitesi, Şanlıurfa, 545–552, 11–13 Şubat (2009b).

Yalman, Y., Erturk, I. “A new histogram modification based robust image data hiding technique”, ***IEEE 24th International Symposium on Computer and Information Sciences (ISCIS’09)***, METU, Northern Cyprus, 39–43, 14–16 September (2009c).

Yalman, Y., Ertürk, İ., “Kişisel bilgi güvenliğinin sağlanmasında steganografi biliminin kullanımı”, ***ÜNAK'09, Bilgi Çağında Varoluş: Fırsatlar ve Tehditler***, Yeditepe Üniversitesi, İstanbul, 1–2 Ekim (2009d).

Yerlikaya, T., Buluş, E., Arda, D., “Asimetrik Kripto Sistemler ve Uygulamaları”, ***II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi***, İstanbul, 24–31, 17–19 Kasım, (2005).

Yılmaz, A., “Robust video transmission”, MSc. Thesis, ***Middle East Technical University***, 2003.

Zhang, X., Wang, S., “Steganography using multiple–base notational system and human vision sensitivity”, ***IEEE Signal Processing Letters***, 12(1), 67–70, (2005).

Zlomek, M., “Video watermarking”, MSc. Thesis, ***Charles University***, (2007).

EK−A: StegVid PROGRAM KODLARI

Tez çalışması kapsamında geliştirilen HSV yönteminin uygulanmasını sağlayan StegVid v1.0 ve v2.0 uygulama yazılımlarına ait program kodları CD içerisinde verilmiştir.

Ancak gömü verilerinin gizlenmesini ve gömülü gizli verilerin çıkartılmasını sağlayan fonksiyonlar CD içerisinde bulunmamaktadır. İlgili fonksiyonların elde edilmesi ve kullanımı için yazar ile irtibata geçilmesi gerekmektedir.

KİŞİSEL YAYINLAR VE PROJELER

A. Uluslararası Hakemli Dergilerde Yayımlanan Makaleler (SCI tarafından taranan)

1. Yalman, Y., Erturk, I., "Secret Data Embedding Scheme Modifying The Frequency of Occurrence of Image Brightness Values", 2010. (Gönderildi)

B. Uluslararası Bilimsel Toplantılarda Sunulan ve Bildiri Kitabında Basılan Bildiriler

1. Yalman, Y., Erturk, İ., "Tarak Etkisi: Veri Gizleme Algoritmalarının İmge Histogramları Üzerindeki Bozucu Etkisi", ***4th International Computer and Instructional Technologies Symposium (ICITS)***, Konya, Turkey, September 24–26 (2010).

2. Yalman, Y., Erturk, İ., Karahan, A., "Gizli Veri Taşıyan Sayısal İmgelerin Tespiti İçin Uygulama Yazılımı Tasarımı", ***4th International Computer and Instructional Technologies Symposium (ICITS)***, Konya, Turkey, September 24–26 (2010).

3. Yalman, Y., Erturk, I. "A New Histogram Modification Based Robust Image Data Hiding Technique", ***IEEE 24th International Symposium on Computer and Information Sciences (ISCIS'09)***, Northern Cyprus, 39–43, 14–16 September (2009).

4. Yalman, Y., Erturk, I., "Bilgisayar Destekli Öğretimde Benzetim (Simülasyon) Kullanımının Öğrenmeye Etkileri", ***3rd International Computer and Instructional Technologies Symposium (ICITS'09)***, Trabzon, Turkey, 1005–1010, October 7–9 (2009).

C. Ulusal Hakemli Dergilerde Yayımlanan Makaleler

1. Yalman, Y., Ertürk, İ., "Sayısal Ses İçerisinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi", ***Politeknik Dergisi***, ***Gazi Üniversitesi,*** 11(4), 319–327, (2008).

D. Ulusal Bilimsel Toplantılarda Sunulan ve Bildiri Kitaplarında Basılan Bildiriler

1. Akbal, T., Yalman, Y., Özcerit, A.T., "Gerçek Zamanlı Sayısal Ses İçerisinde Sıkıştırılmış ve Şifrelenmiş Veri Transferi", ***III. Ağ ve Bilgi Güvenliği Sempozyumu***, Çankaya Üniversitesi, Ankara, 5–6 Şubat (2010).

2. Yalman, Y., Ertürk, İ., "Kişisel Bilgi Güvenliğinin Sağlanmasında Steganografi Biliminin Kullanımı", ***ÜNAK'09, Bilgi Çağında Varoluş: Fırsatlar ve Tehditler***, Yeditepe Üniversitesi, İstanbul, 1–2 Ekim (2009).

3. Yalman, Y., Ertürk, İ., "İmge Histogramı Kullanılarak Geometrik Ataklara Dayanıklı Yeni Bir Veri Gizleme Tekniği Tasarımı ve Uygulaması", ***XI. Akademik Bilişim Konferansları***, Harran Üniversitesi, Şanlıurfa, 537–544, 11–13 Şubat (2009).

4. Yalman, Y., Ertürk, İ., "Gerçek Zamanlı Video Kayıtlarına Veri Gizleme Uygulaması", ***XI. Akademik Bilişim Konferansları***, Harran Üniversitesi, Şanlıurfa, 545–552, 11–13 Şubat (2009).

5. Yalman, Y., Ertürk, İ., "Sayısal Ses İçerisinde Gizli Metin Transferinin Kablosuz Ortamda Gerçekleştirilmesi", ***Ulusal Teknik Eğitim, Mühendislik ve Eğitim Bilimleri Genç Araştırmacılar Sempozyumu (UMES'07)***, 41–45, 20–22 Haziran (2007).

E. Görev Aldığı Projeler

1. Araştırmacı***, Sayısal İmge İçerisine Yeni Bir Veri Gizleme Yöntemi Tasarımı,*** KOÜ, Bilimsel Araştırma Projeleri Birimi, 2009/044, 2009–2010.

ÖZGEÇMİŞ

Yıldıray YALMAN, 1981 yılında Kocaeli ilinde doğdu. İlköğrenimini çeşitli illerde okuduktan sonra, lise eğitimini Kocaeli Teknik Lisesi Bilgisayar Bölümü'nde tamamladı. 1999 yılında girdiği Kocaeli Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi Bölümü Bilgisayar Öğretmenliği programından 2004 yılında sınıf birinciliği ve bölüm üçüncülüğü derecesi ile Bilgisayar Teknik Öğretmeni olarak mezun oldu. 2004–2007 yılları arasında Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim Dalı'nda Yüksek Lisans öğrenimini tamamladı. Aynı yıl başladığı Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim Dalı'ndaki doktora programına halen devam etmektedir. 2004–2005 yıllarında Hereke Nuh Çimento Anadolu Teknik Lisesi, Teknik Lise ve Endüstri Meslek Lisesi'nde Bilgisayar Öğretmeni olarak görev yaptı. 2006 yılından itibaren Ümraniye Ticaret Meslek Lisesi'nde Bilişim Teknolojileri Öğretmeni olarak görev yapmaktadır. Evli ve bir çocuk babasıdır.